CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6510.01B
22 August 1997

DEFENSIVE INFORMATION OPERATIONS IMPLEMENTATION

References: Enclosure E.

1. Purpose. To provide implementing guidance and supplemental joint policy for defensive information operations (IO) in accordance with references a-ff.

2. Cancellation. CJCSI 6510.01A, 31 May 1996, “Defensive Information Warfare Implementation,” is canceled.

3. Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, and joint and combined activities.

4. Introduction. Defensive IO concepts are described in Enclosure A.

5. Policy. In addition to policy guidance in reference a, the following is the Chairman of the Joint Chiefs of Staff’s specific defensive IO policy guidance.

a. Information, information-based processes, and information systems (such as command, control, communications, and computer (C4) systems, weapon systems, and infrastructure systems) used by US military forces will be protected relative to the value of the information contained therein and the risks associated with the compromise of or loss of access to the information.

b. Information system defense relies on four interrelated processes. These include a process to protect information and information systems, a process to detect attacks or intrusions, a restoration process to mitigate the effects of incidents and restore services, and a response process.

Additionally, offensive actions can play an integral role in the defensive process by deterring adversary intent to employ IO capabilities and/or neutralizing adversary IO capabilities. Information system defense capabilities will be incorporated into information systems and employed continuously across the range of military operations.

c. Policy. See Enclosure B.

6. Definitions. See reference gg and Glossary.

7. Responsibilities. See Enclosure C.

8. Procedures. See Enclosure D.

9. Summary of Changes. This revision:

a. Broadens the scope of the instruction from defensive information warfare to defensive IO.

b. Updates information from the canceled documents.

10. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

\Signature\
DENNIS C. BLAIR
Vice Admiral, U.S. Navy
Director, Joint Staff

Enclosures:
A -- Introduction
B -- Policy
C -- Responsibilities
D -- Procedures
E -- References
Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Secretary of Defense	10
Director of Central Intelligence	2
President, National Defense University	25
Commandant, Armed Forces Staff College	5
Commander, US Element, NORAD	5
Commander, US Forces Korea	5
Commander, Joint Communications Support Element	10
Director, Joint Command and Control Warfare Center	10
Director, Joint Spectrum Center	5
Director, Joint Warfighting Center	10

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6510.01B. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	D-B-A-1 thru D-B-A-8	O
i thru viii	O	D-C-1 thru D-C-2	O
A-1 thru A-16	O	D-C-A-1 thru D-C-A-2	O
B-1 thru B-10	O	D-D-1 thru D-D-2	O
C-1 thru C-12	O	D-E-1 thru D-E-4	O
D-1 thru D-2	O	D-F-1 thru D-F-4	O
D-A-1 thru D-A-4	O	D-G-1 thru D-G-4	O
D-A-A-1 thru D-A-A-2	O	D-H-1 thru D-H-2	O
D-A-B-1 thru D-A-B-2	O	E-1 thru E-4	O
D-A-C-1 thru D-A-C-2	O	GL-1 thru GL-16	O
D-B-1 thru D-B-2	O		

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE Page

ENCLOSURE A

INTRODUCTION

1. General. Warfighters depend upon information to plan operations, deploy forces, and execute missions. Information systems serve as an enabler and enhance warfighting capabilities. However, increasing dependence upon rapidly evolving technologies makes joint forces more vulnerable. Defensive information operations (IO) ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives. Four interrelated processes comprise defensive IO: information environment protection, attack detection, capability restoration, and attack response. The defensive IO processes integrate all available capabilities to ensure defense-in-depth. Offensive actions can play an integral role in the defensive process in that they can deter adversary intent to employ IO and/or neutralize adversary IO capabilities. Defensive IO integrates and coordinates protection and defense of information, information-based processes (including human decision-making processes), and information systems (including command, control, communications, and computer (C4) systems, weapon systems, and critical information infrastructure systems, etc.). The defensive IO process is an integral part of deterrence and force protection. This enclosure describes defensive IO concepts. Other elements of this instruction provide policy (Enclosure B), responsibilities (Enclosure C), and procedural guidance (Enclosure D) for implementing defensive IO. Reference a addresses all aspects of IO for consideration when planning and implementing defensive IO.

2. Defensive IO Process. Defensive IO are conducted through information assurance (IA), physical security, operations security, counter deception, counter psychological operations, counter intelligence, and electronic protect. Offensive actions can also support the defensive process. Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes. Information assurance ensures the availability, integrity, identification and authentication (I&A), confidentiality, and non-repudiation (see Glossary for definitions of these terms) of US Government information. Figure 1 on page A-2 illustrates the elements of the target set of information and information systems protected and defended by defensive IO processes.

a. Information (defined in Glossary) exists in a variety of formats from human senses to electronic and written formats.

b. Information systems (automated and manual) (defined in Glossary) are composed of three basic elements or components: information transfer links, information processing nodes (including information storage), and human factors.

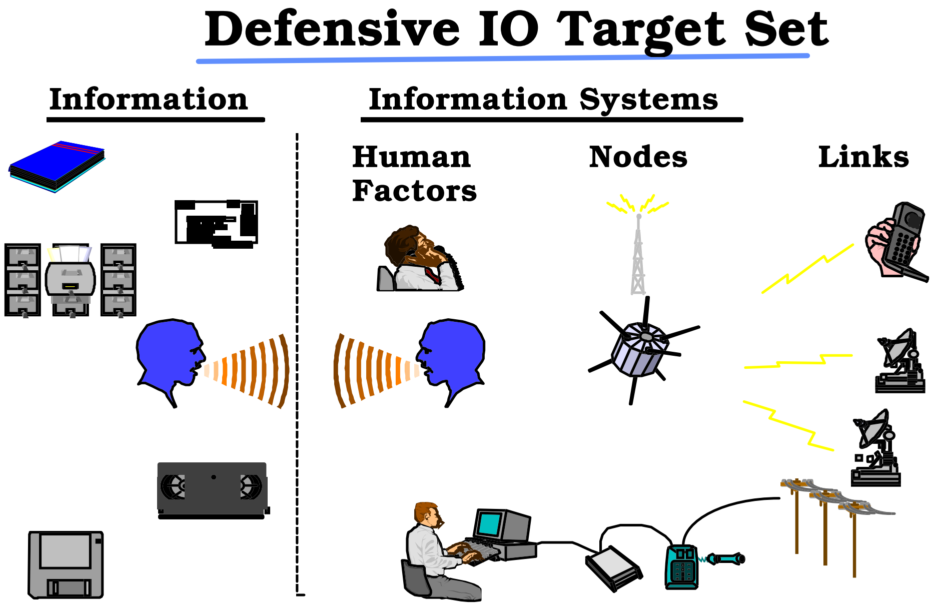

Figure 1 - Information and Information Systems: The Target Set

3. <u>Defensive IO and C2 Systems</u>

a. Defensive IO focuses on the protection and defense of information systems (including C2 systems, weapons systems, and communications systems). While C2 systems are all considered information systems, not all C2 systems are considered automated information systems (AISs). A point-to-point radio link may be a C2 system, but not necessarily an AIS.

b. Similarly, not all information systems or AISs are considered C2 systems. For example, an intelligence radio net is an information system, but not necessarily a C2 system. Similarly, a medical logistics AIS is not considered a C2 system.

c. Joint forces rely on effective C2 for conducting operations. C2 is a subset of the IO target set (information, information-based processes, and information systems). However, the target set's integrated nature makes traditional distinctions between individual systems based strictly on function (such as C2) an outmoded and ineffective methodology. In practice, a variety of telecommunications systems and AISs, not all traditionally considered C2 systems, process information with C2 application and value. Effective protection of friendly C2 relies on protecting information with C2 value, independent of system function and where the information is present. Protection of C2 capability requires an integrated defensive IO approach based on the value of information. Reference kk describes some, but not all, C2-protection policy.

4. Technology Impact

a. Widespread use of modern information technology has led to dependence on computers and software. Integration of telecommunications and AIS is commonplace and obscures previously distinct disciplines. The DOD's reliance on telecommunications and AIS (including hardware and software) continues to increase. As the degree of overlap increases between these disciplines, understanding operational requirements becomes more difficult. Knowledge sharing between information disciplines will ensure warfighting requirements are addressed.

b. Information systems technology is advancing rapidly, including specific technologies used to attack, protect, and defend systems. Within many of these technologies are vulnerabilities which create requirements for defensive IO.

c. Dependence on vulnerable technologies introduces risk. The need to manage this risk and mitigate vulnerabilities is a major impetus behind defensive IO.

5. Reachback Dependencies. Warfighters at all levels should understand the nature, complexities, and dependencies the global information infrastructure (GII), national information infrastructure (NII), and defense information infrastructure (DII) have during the various phases of an operation across the range of military operations.

a. The successful conduct of operations in the information age requires access to information available outside the operational area. Information infrastructures (including critical infrastructures) no longer parallel traditional command lines, and warfighters need frequent, instant, and reliable access to information at locations in the continental United States (CONUS) as well as in theater. For example, mobility and sustainment of forces are highly dependent on commercial "reachback" infrastructures that include international telecommunications, the public switched network, transportation systems, and commercial electric power grids. Joint Forces require secure video teleconferencing, database connectivity, and broadcast/receive capabilities for reachback access to intelligence, logistics, and other essential support data. The technical complexity and management of these information infrastructures inhibits a commander's ability to control the flow of information or dynamically manage available information and telecommunications resources. (see glossary for definition of critical infrastructures)

b. Supporting crises and contingency operations requires the rapid expansion of C4 capabilities beyond their normal peacetime limits. Joint forces must have assurance that this expanded C4 infrastructure can attain the level of protection required to assure mission success. The implementation of this or any other level of protection for the NII requires the cooperative efforts of service providers, the Department of Defense, and government.

c. Our dependence on information and information systems and the exposure of our vulnerabilities to a wide range of threats, from computer hackers through criminals, vandals, and terrorists to nation states, have brought focus and compelling relevance to the emerging discipline of defensive IO. Its unique characteristics set in motion revolutionary capabilities that will enhance and support warfighting into the next century.

6. Elements of the Defensive IO Process. Defensive IO occurs within the context of four interrelated processes: information environment protection, attack detection, capability restoration, and attack response. Figure 2 on page A-5 illustrates the defensive IO implementation process. The following paragraphs describe these processes.

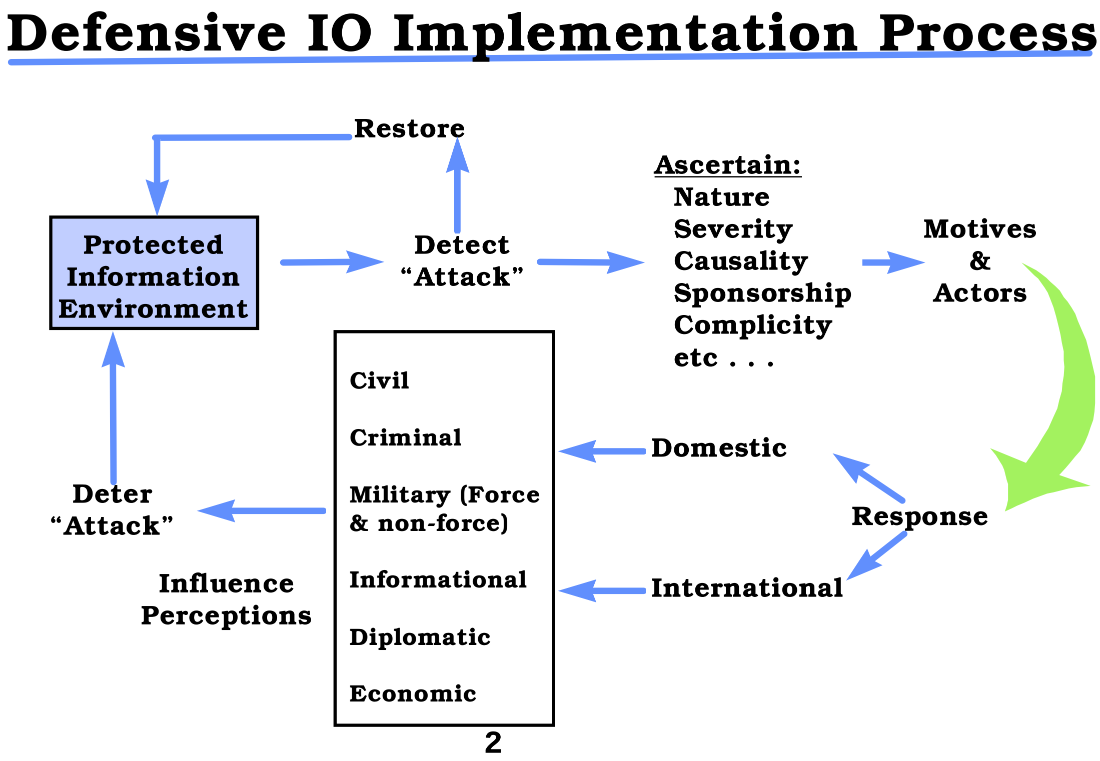

Figure 2 - Defensive IO Implementation Process

a. Information Environment Protection Process. Information protection is critical to the military's ability to conduct operations and is the responsibility of leaders, information producers, processors, and users. Information protection applies to any medium and form including hardcopy (message, letter fax), electronic, magnetic, video, imagery, voice, telegraph, computer, human, etc. Information protection ensures availability, integrity, authenticity, confidentiality, and nonrepudiation of information. The information protection process (Figure 3 on page A-6) involves determining the scope (what to protect based on the value of information) and the standards for protection (to what extent through operations and the application of protective measures and technologies). The protection process should reflect the changing value of information during each operational phase.

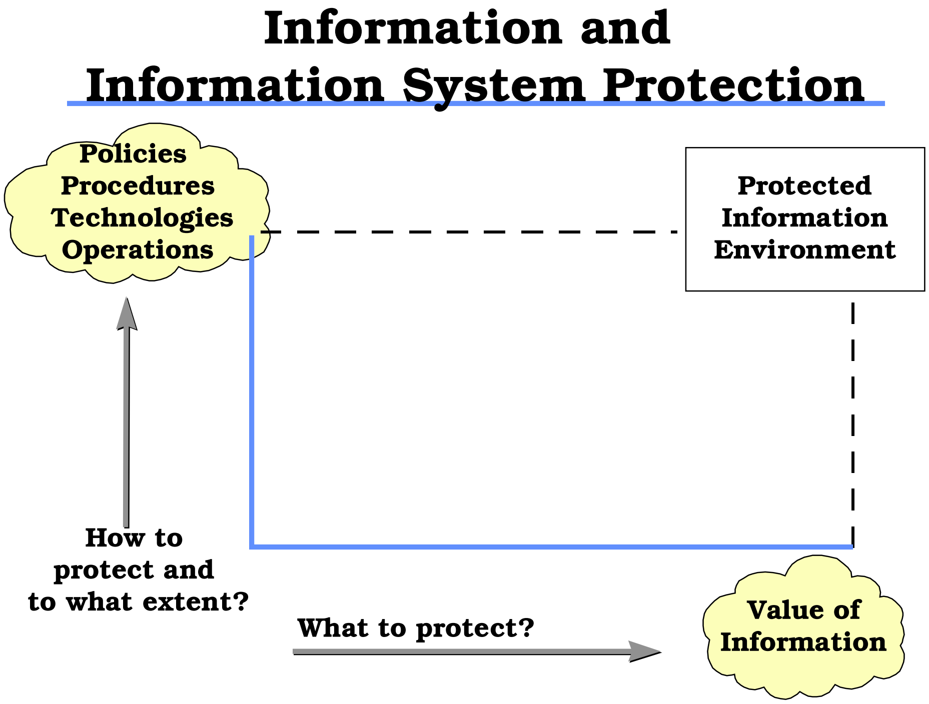

Figure 3 - Information and Information System Protection

(1) Policies

(a) National level information and information system protection policies come in many forms. Included are policies created by organizations such as the Office of Management and Budget (OMB) (reference b), the National Security Telecommunications and Information Systems Security Committee (NSTISSC) (references c - t), and the Security Policy Board (SPB). Also included are Public Laws (reference u), Executive Orders, and Presidential directives (reference v). Many of these policies, as well as Department of Defense (DOD) policy documents (references w - cc, and reference aaa), are directive and provide guidance to the Chairman of the Joint Chiefs of Staff (CJCS). This instruction implements those policies. See Enclosure B.

(b) National policy scope is very broad, ranging from application of specific vulnerability countermeasures to technology transfer constraints. The latter includes identifying and controlling technology export having IO applications and contributes to information protection by restricting access to tools useful for attacking our information systems.

(2) Capabilities and Procedures. Use of common capabilities and procedures contribute directly and indirectly to information protection, information systems security (INFOSEC), and information systems protection. See Enclosure D.

(a) Information Assurance. Information assurance capabilities help ensure the availability, integrity, identification and authentication, and confidentiality, and nonrepudiation of friendly information and information systems while denying adversary access to the same information and information systems. IA is a life cycle process that begins with requirements identification and continues through system design, acquisition, fielding, training, implementation and operation, and modification or upgrade. IA capabilities are incorporated into information systems at the beginning of the acquisition cycle and employed throughout the life cycle. IA capabilities include, but are not limited to, technical security measures such as INFOSEC devices.

(1) INFOSEC. INFOSEC is the protection of information systems against unauthorized access or modification of information, whether storage, processing or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of the following two disciplines:

(2) COMPUSEC. COMPUSEC involves the measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

(3) COMSEC. COMSEC includes measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security (TRANSEC), emission security, and physical security of COMSEC material.

(b) Security. Personnel security and physical security measures are examples of procedures contributing indirectly to information protection.

(c) Operations Security (OPSEC). OPSEC is a process that identifies critical information and subsequently analyzes friendly actions attendant to military operations and other activities, and then implements procedures to prohibit disclosure of critical information to an adversary.

(d) Counterdeception. Activities contributing to awareness of adversary posture and intent also serve to identify adversary attempts to deceive friendly forces.

(e) Counterpsychological operations. Activities identifying adversary psychological warfare operations contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces.

(f) Counterintelligence (CI). CI activities integrate and coordinate protection and defense of information and information systems. CI support to defensive IO includes collection focused on I&W and the identification of threats to information and information systems; investigations of computer-based crimes; and analysis of production support to policy, plans, operations, acquisition, and force protection.

(g) Electronic Warfare (EW). Defensive EW procedures known as electronic protection (EP), including communications security (COMSEC) procedures, changing call signs/words and frequencies, antenna and communications site positioning, are examples of procedures/disciplines directly contributing to information and information system protection. Others include computer security (COMPUSEC) procedures, operations security (OPSEC), and personnel information access controls.

(h) Education, Training, and Awareness. A key component for success in information protection is education and training of information and information system users, administrators, managers, engineers, designers, and requirements developers. Awareness heightens threat appreciation and the importance of adhering to protective measures. Education provides the concepts and knowledge to develop appropriate technologies, policies, procedures, and operations to protect systems. Training develops the skills and abilities to mitigate system vulnerabilities, and implement and maintain protected systems.

(i) Risk Management. Risk management decisions determine limits for applying countermeasures. Risk management includes consideration of information needs, the value of information at risk, system vulnerabilities, threats posed by potential adversaries and natural phenomena, and resources available for protection and defense. Procedures and actions to minimize loss or degradation of information, once discovered, are also an important part of risk-management.

(j) Intelligence. Intelligence is an important element in the protection process. The nature of intelligence requires that it, too, must be adequately protected. Intelligence provides an understanding of the threat to information and information systems by identifying potential information adversaries, their intent, and their known and assessed capabilities. Threat information is a key consideration in the risk management process.

(k) Public Affairs and Command Information. Public affairs and command information programs contribute to information protection by disseminating factual information. Factual information dissemination counters adversary deception and psychological operations (PSYOP).

(l) Vulnerability Analysis and Assistance. Friendly forces conduct vulnerability analyses and assistance to identify vulnerabilities in information systems and to provide an assessment of their effects on information access and availability. This analysis is a key consideration in the risk management process.

1. Threats to information systems are broader than those posed by adversaries. Internal threats, malicious and accidental, pose perhaps the most significant threat to systems. Natural phenomena such as sunspots, hurricanes, tornadoes, fires, earthquakes, and floods also pose risks to systems. Vulnerability analysis of systems must include consideration of these factors as well.

2. Vulnerability analysis and assistance efforts focus on specific types of information systems. For example, the Defense Information Systems Agency (DISA) operates a program known as the Vulnerability Analysis and Assistance Program (VAAP) specifically focusing on AIS vulnerabilities. The Services and CINCs also operate similar vulnerability assessment programs.

The National Security Agency (NSA) has a COMSEC monitoring program that focuses on telecommunications systems using wire and electronic communications.

3. CI, personnel, physical, and facility security surveys are additional measures designed to determine and probe organizational IO vulnerabilities. Coordinated application of all these activities provides the organization a more complete vulnerability assessment and assists in risk management.

4. There are four types of vulnerability assessments:

a. Assessments at the initial design phase of an information intensive system. The program manager tracks this assessment throughout the life cycle of the system.

b. Assessments during the testing phase to determine inadvertent vulnerability design and incorporation.

c. Assessments after system fielding to ensure proper security feature operation.

d. Assessments made during system operation.

(3) Defensive Operations. Operations with an objective of deterring or, when deterrence fails, defeating specific threats to information or information systems contribute directly to defensive IO objectives. Operations conducted for purposes other than defeating IO threats also may have collateral effects supporting defensive IO objectives. Offensive actions can support defensive objectives by deterring adversary intent to employ IO and/or neutralize adversary IO capabilities. These actions can be preemptive or in response to adversary IO attacks.

(a) Offensive actions can be conducted to support defensive IO throughout the range of military operations. Offensive actions must be integrated with defensive IO to provide timely response against identified and potential threats to friendly information and information systems.

(b) Selection and employment of specific offensive IO capabilities must be consistent with US objectives, applicable international conventions, and rules of engagement.

b. Attack Detection Process. The attack detection process requires close cooperation/coordination among information system developers, vendors, incident response teams, impacted corporate entities, administrators and users, service providers, civilian and military law enforcement, and intelligence agencies. This process also includes detecting deception and psychological operations conducted against friendly forces. The speeds at which IO attacks occur, in many cases, have outpaced our ability to detect and respond via human means. An automated method to assess the severity (including system damage, information compromise, and malicious logic insertion) and to mitigate these effects is essential to effective defensive IO. Timely detection and reporting of IO attack is key to initiating the restoration and response processes. Some elements of the IO attack detection process for information systems include the following:

(1) Information System Developers. Information system developers must be knowledgeable of vulnerabilities inherent in technology and the operational employment and integration of systems. Systems must be designed and fielded in a manner that mitigates those vulnerabilities and detects attempts to exploit those vulnerabilities. The speeds involved in AIS attacks dictate automatic detection, mitigation, and reporting mechanism inclusion in system design.

(2) Information System Providers and System Administrators. New information system attack techniques emerge over time. Even the best designed system is subject to emergent attack capabilities. Providers and administrators must be capable of recognizing abnormalities in system functioning and take appropriate action to report and mitigate the effects of adversary actions. They must establish a system for periodic risk assessment and detection/mitigation system updates.

(3) Information and System Users. Users exposed to information may be able to detect content differences. Users must be aware of potential threats to and the vulnerabilities inherent in their media. This includes the adversary's use of information as part of a deception or PSYOP campaign. Users recognizing abnormalities or unexplained changes in content, or disturbed information files or media, must also be proficient in employing procedures for safeguarding evidence and reporting incidents.

(4) Law Enforcement. Detection of information system incidents or intrusions may occur as collateral information obtained by law enforcement during criminal investigations. This type of information must be shared with the affected systems administrators, the intelligence community, system developers and, as necessary, with the producers and users of affected information or information systems. Internal procedures should facilitate criminal or counterintelligence investigations of the incident while protecting the integrity of the information or information system as well as protecting individual privacy rights. Services and commands must develop procedures to determine conditions and mechanisms for reporting to law enforcement.

(5) Intelligence. Intelligence contributes to attack detection by establishing and collecting against specific activity indicators and by providing warnings of potential adversary activity. Close coordination is required between intelligence, law enforcement, system developers, providers, administrators, and users to ensure sharing of relevant information. Intelligence and C4 processes form the foundation for indications and warning.

(a) Indications and Warning (I&W). I&W for defensive IO draw from current intelligence reports, organic joint force assets, combatant command I&W support, and correlation of force movements in a commander's area of responsibility. In addition, national-level intelligence assets provide I&W of imminent adversary activity.

(b) Defending against any IO attack depends on how well the intelligence threat and associated I&W processes function and on the agility of systems providers, users, and administrators to implement protective countermeasures.

(6) Reporting Structure. Systems should be designed to alert managers and administrators at all levels of abnormalities. Timely collation, correlation, information analysis, and warning dissemination require a continuously functioning reporting structure. Automated analyses and alerts of attacks in progress are essential to the detection process. The structure must be linked to intelligence, law enforcement, policy makers, and the information systems community (both government and commercial). Attack reporting procedures must consider the information needs of the acquisition, intelligence and operations communities for planning, coordinating, and implementing response options. Reporting procedures are at Enclosure D.

c. Capability Restoration Process. The capability restoration process relies on established mechanisms for prioritized restoration to minimum essential capabilities (reference hh).

(1) Capability restoration may rely on backup/redundant links or system components, backup data bases, or even alternative means of information transfer. Information system design and modification must consider incorporating automated restoration capabilities and other redundancy options.

(2) In some cases, required technical restoration capabilities are beyond the abilities of the affected sites. On-line or deployable restoration assistance capabilities provide required expertise and tools to restore services. Common types of restoration assistance are the computer emergency response team (CERT) and security incident response capability (SIRC). DISA, the Services, unified commands, and commercial establishments have CERT and/or SIRC-type programs.

(3) Automated alerting mechanisms provide system managers and administrators with enhanced situational awareness and create decision points. Immediate termination of adversary system access to protect against further actions and information exploitation must be weighed against the needs of the legal and intelligence communities to collect against and exploit the adversary. The system owner, system designated approving authority (DAA), or higher authority must decide whether or not to allow an intruder to maintain access in order to gather information for the response process. The decision must rely on a risk assessment of continued access, consideration of current and future operations, and intelligence impact.

(4) A key step in the restoration process is to inventory system and information resources to identify surreptitious adversary implants.

(5) Finally, post attack analysis provides information about vulnerabilities exploited and leads to security improvements. Automated recording or capturing of specific attack techniques during an incident can provide information required for analysis.

d. Attack Response Process. The attack response process involves determining actors and their intent, establishing cause and complicity, and possibly appropriate action(s) against perpetrators. The process contributes to information environment protection by removing threats and enhancing deterrence. Elements of the IO attack response may include national-strategic decisions to apply flexible deterrent options, either stand alone or in parallel. Possible response options could include the following:

(1) Law Enforcement. Law enforcement can contribute to information protection by imprisoning criminals. Imprisoning criminals may deter other criminals/adversaries conducting attacks on information systems.

(2) Diplomatic Actions. Diplomatic actions can provide a powerful deterrent without resorting to lethal force. Diplomatic actions can be taken at low cost, are scaleable, and are easily changed.

(3) Economic Sanctions. Economic sanctions offer another alternative to military force. Economic sanctions have a number of weaknesses, however, including enforcement, which often relies on military force.

(4) Military Force. Military force is a response option that directly eliminates the threat, or interrupts the means or systems that an adversary uses to conduct an attack.

(5) While the attack response process is integral to defensive IO, additional details are beyond the scope of this instruction.

7. Education, Training, and Awareness. Information and information systems are placed at risk when persons responsible for system security oversight or management are unaware of responsibilities, procedures, and techniques for protecting their systems. Defensive IO is multidisciplinary, requiring a wide spectrum of knowledge such as OPSEC, emanations security, physical security, personnel security, and related security areas. Recognizing the convergence and interdependence of traditional telecommunications and AIS technology is a necessity. Basic defensive IO education, training, and awareness are security countermeasures. References a and w address IO education and training.

8. Joint and Multinational Interoperability. Military forces employed in joint and multinational operations are challenged with creating a secure, interoperable information environment satisfying warfighting information requirements.

a. Programs such as the Joint Staff Intertheater COMSEC Package (JSICP) program (reference ii), the COMSEC Utility Program (CUP), the COMSEC Coalition Pool, and processes for releasing COMSEC equipment to allies create the secure allied/coalition information environment.
This environment, however, presents challenges to information producers, managers, and users to ensure the proper release, handling, and access to information.

b. Implementing defensive IO capabilities for networked systems in this environment is even more challenging. Protection, detection, restoration, and response across multinational systems, political boundaries, and electronic boundaries present special challenges.

(INTENTIONALLY BLANK)

POLICY

1. General

a. Information, information-based processes, and information systems such as: command, control, communications, and computer (C4) systems; weapon systems; and information infrastructures used by US military forces will be protected relative to the value of the information contained therein and the risks associated with its compromise or loss.

b. Information system defense relies on four interrelated processes. These include a process to protect information and information systems, a process to detect attacks or intrusions, a restoration process to mitigate the effects of incidents and restore services, and a response process. Information systems will incorporate information system defense capabilities and employ them continuously across the range of military operations.

c. Joint IO doctrine, once developed, will provide guidance for integrating defensive IO processes, procedures, and capabilities in support of military operations.

d. Reference a provides a recommended mechanism for inclusion in future joint doctrine for accomplishing IO coordination and integration.

2. Information Protection

a. The DOD Information Security and Personnel Programs (references u, v, x, y, and z) provide policy for information protection and personnel security. Information warranting protection against unauthorized disclosure will be properly classified and safeguarded. In addition to having the required security clearance to access classified material, individuals who access information and information systems must be assigned to one of the three position sensitivity designations listed in appendix K of reference z.

b. Transmitting classified national security information requires secure means.

c. Sensitive information must be protected during transmission, processing, and storage to the level of risk, loss, or harm that could result from disclosure, loss, misuse, alteration, intentional or inadvertent destruction, or nonavailability. The cognizant DOD component head or designated representative will determine the appropriate level of protection for sensitive unclassified information.

d. Disclosure of classified military information to foreign governments and international organizations will be IAW references cc and dd.

e. OPSEC contributes to information protection. Reference jj promulgates OPSEC policy.

f. The defensive aspects of EW, known as EP, also contribute to information protection. Reference kk promulgates EW policy.

3. Information System Protection

a. Telecommunications and Information Systems Protection (references h, v, and bb)

(1) Threat and Vulnerability Assessment. Threat and vulnerability assessments must be conducted for all telecommunications and information systems used for processing, storing, and transmitting classified, sensitive unclassified, and unclassified national security-related information.

(2) Classified Information

(a) National security systems (see Glossary), including those operated and maintained by US Government contractors, must be protected to prevent unauthorized access, denial of service, compromise, tampering, or exploitation of information.

(b) Authorized products and services (e.g., NSA-endorsed) and/or certified and accredited systems must be used to protect national security telecommunications and information systems.

(3) Sensitive Unclassified Information

(a) Sensitive unclassified information must be safeguarded so that only authorized persons have access, it is used only for its intended purpose, it retains content integrity, and it is properly marked.

(b) Sensitive information subject to reference u may be protected during transmission, processing, and storage by products validated as meeting applicable Federal Information Processing Standards or by NSA-endorsed COMSEC products, techniques, and protected services.

(4) Unclassified Information

(a) Unclassified information transmitted by and between US military forces and contractors will be protected against tampering, loss, and destruction commensurate with the associated risk of its exploitation.

(b) Except in prescribed instances, military forces may procure and use commercial cryptographic equipment and techniques to satisfy communications protection requirements for unclassified information. NSA approved equipment must be used if the function, operation, or use of the equipment involves the command and control of military forces or is critical to the direct fulfillment of military intelligence missions.

(c) Suggested safeguards for unclassified information are outlined in reference b and include applicable personnel, physical, administrative, and technical controls.

(5) Controlled Access Protection (reference p). All AISs accessed by more than one user, when those users do not have the same access authorization or need, must provide automated controlled access protection for all classified and sensitive unclassified information.

(6) Certification and Accreditation (C&A) of National Security Telecommunications and Information Systems (reference m). The DOD components will ensure certified and accredited information systems are fielded to the warfighter. C&A programs ensure adequate protection for information processed, stored, or transmitted by national security systems. The following principles are the basis of C&A programs established to satisfy this policy:

(a) Certification of national security systems will be performed and documented by appropriate personnel in accordance with specified criteria, standards, and guidelines (see Enclosure D).

(b) Accreditation of national security systems will be performed by appropriate management personnel in a position to balance operational mission requirements and the residual risk of system operation. Accreditation decisions will be documented and contain a statement of residual risk.

(c) Military forces should freely exchange technical C&A information, coordinate programs, and participate in cooperative projects.

(d) Programs for the C&A of national security systems must be developed in concert with similar programs addressing sensitive information security pursuant to reference u in order to promote cost-effective security.

(e) C&A shall be performed at appropriate points throughout the system life cycle. This should include periodic or event-related risk assessments during the system's operational life.

(f) Interim approval to operate systems being developed may be granted by the accreditation authority provided appropriate safeguards are specified pending full accreditation.

b. Voice Communications Protection (reference g).

(1) All military voice radio systems must be protected consistent with the information transmitted on the system, to include cellular and commercial services. Priorities will be established based on an assessment of threats to and vulnerabilities of specific systems.

(2) Military voice radio systems used to transmit classified information must be protected with approved security services and/or equipment.

c. Data Services Protection (reference n). All unclassified systems used by DOD are considered sensitive but unclassified (SBU). These systems will be protected by tools that ensure user identity and authentication. Additionally, privacy act data will be protected during transmission. All SBU systems will implement adequate network countermeasure tools, including system monitoring, attack detection, fault and intruder isolation, and automated attack mitigation. Classified systems will incorporate transmission encryption in addition to identification, authentication, and network countermeasure tools.

d. Control of Compromising Emanations (references q and aa)

(1) Military forces and their designated agents shall use TEMPEST countermeasures in proportion to the threat and associated potential damage to the national security. In accordance with references t and aa, a Certified TEMPEST Technical Authority (CTTA) must conduct or validate all TEMPEST countermeasure reviews. Provisions of this policy apply to national security systems, to US military forces, and operations worldwide.

(2) TEMPEST Countermeasure Application in CONUS. Within the US, critical information will be protected by emanations countermeasures in accordance with references aa and zz.

e. COMSEC

(1) COMSEC Material Control System (CMCS) (reference c). It is US Government policy to encourage COMSEC material and technique use and to safeguard COMSEC materials in a manner assuring continued integrity, prevention of unauthorized access, and controlling of the spread of COMSEC materials, techniques, and technology when not in the best interest of the US and its Allies. Implementation of this policy requires each department and agency holding COMSEC keying material establish a CMCS into which all COMSEC keying material will be placed. Other COMSEC material may be placed in the CMCS or any other material control system providing the requisite security and management control.

(2) Electronic Keying (reference k). Electronic keying programs will be established and implemented with the objective of replacing dependence on paper-based/nonelectronic keying methods by the year 2000. Electronic keying will be applied to all cryptographic processes related to national security systems.

(3) Application of COMSEC to US Civil and Commercial Space Systems (reference i)

(a) Classified national security information transmitted over satellite circuits must be protected by approved techniques from unauthorized intercept.

(b) Use of US civil (Government-owned but non-DOD) and commercial satellites launched since June 1990 will be limited to space systems using accepted techniques to protect the command/control uplinks.

(4) Selection and Protection of Machine Cryptosystems for use in High Risk Environments (reference e)

(a) Machine cryptosystems for use in high risk environments will be selected taking into consideration the factors promulgated by the Director, NSA. High risk environments for machine cryptosystems will be identified in accordance with standardized criteria (reference ll).

(b) In all high risk environments, a workable contingency plan should be developed to guide protection, evacuation, or destruction of COMSEC equipment and other COMSEC materials should they become jeopardized.

(c) Only the minimum amount of mission essential COMSEC material may be located in high risk environments.

(d) In accordance with reference e, only approved keying material will be used for secure communications to and from high risk areas.

(5) Granting Access to US Classified Cryptographic Information (reference j). Certain US classified cryptographic information requires special access controls. Access to this information must only be granted to individuals satisfying specific criteria (see Enclosure D).

(6) Release of COMSEC Information to US Nongovernmental Sources (reference d). COMSEC operations normally will be conducted by the government. Military forces may obtain required COMSEC support from, and may provide COMSEC information and material to, US nongovernmental sources within limitations outlined in Enclosure D.

(7) Disclosure or Release of COMSEC Information to Foreign Governments and International Organizations (references f and dd). The disclosure or release of US COMSEC information to foreign governments or international organizations will be done only when determined to be in the best interest of the US Government. Procedures for determining responses to release requests (Enclosure D) require consideration of risks resulting from disclosure or release.

(8) COMSEC Monitoring (reference s). US Government departments and agencies conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to government telecommunications and aid in countering their vulnerability.

(a) US military forces conducting COMSEC monitoring activities must be in strict compliance with the law, Executive orders, applicable Presidential directives, and this instruction.

(b) Government telecommunications systems are subject to COMSEC monitoring by duly authorized government entities (as specified by individual department or agency regulations). Users of these systems must be properly notified in advance, in accordance with guidelines in Enclosure D, that system usage constitutes implied consent to monitoring for COMSEC purposes. Note: Consent to COMSEC monitoring is required of only one party to a conversation or transmission.

(c) Military forces will not monitor telecommunications systems owned or leased by government contractors for their own use without first obtaining the expressed written approval of the contractor’s chief executive officer (or his/her designee) and the written opinion of the department or agency general counsel actually performing the monitoring.

(d) Military forces will not monitor for COMSEC purposes the contents of telecommunications when such monitoring constitutes electronic surveillance.

(e) In accordance with procedures approved by the Attorney General, information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring relating directly to a significant crime will be referred to the military commander or law enforcement agency having jurisdiction.

When taking such action, the general counsel of the department or agency performing the COMSEC monitoring will be notified promptly. COMSEC monitoring results may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency performing the monitoring.

(f) COMSEC monitoring results will not be used to produce foreign intelligence or counterintelligence as defined in reference mm. However, the results of COMSEC monitoring of US and Allied military exercise communications may be used for intelligence purposes under procedures prescribed in applicable directives.

(g) No department or agency may monitor another department or agency's telecommunications for COMSEC purposes without the expressed prior written approval of the head (or his/her designee) of the department or agency to be monitored, except as provided for in Enclosure D.

(h) COMSEC monitoring will be conducted in strict accordance with operational procedures minimizing the possibility that unnecessary communications content will be acquired. Such procedures will be consistent with guidelines approved in writing by the general counsel of the department or agency issuing the procedures.

(i) This policy is applicable to US Military Departments and agencies engaged in or using the results of COMSEC monitoring. Reference s is approved by the Attorney General. References nn, oo, and pp are pertinent to COMSEC monitoring guidelines and procedures. Technical surveillance countermeasures, electronic sweeps, surveillance of noncommunications emissions (e.g., radar), and TEMPEST testing are not within the scope of COMSEC monitoring.

4. Information System Defense

a. Incident Response and Vulnerability Reporting for Information Systems (reference l). Events involving the use of international telecommunications and computer systems to exploit and disrupt information systems clearly underscore the need for an organized and fully supported capability to deal with such incidents. Accordingly, US military forces should collaborate and coordinate efforts to:

(1) Contain and minimize the impact of security incidents on information systems.

(2) Report incidents and mitigate vulnerabilities in information systems (see Enclosure D).

b. Changing Call Signs/Words and Frequencies. CJCS policies for changing call signs/words and frequencies are addressed in reference ff.

5. Defensive IO Education, Training, and Awareness (references a, r, and w)

a. References a and w address IO education.

b. Education, training, and awareness programs addressing defensive IO are being developed under the auspices of the Inter-Service Training Review Organization Initiative for Joint IO Training, and the DOD Education, Training, and Awareness, and Professionalization Working Group.

c. It is national policy that US Government departments and agencies develop and implement INFOSEC education, training, and awareness programs for national security systems. This policy is applicable to US Government departments and agencies, their employees, and contractors.

(1) INFOSEC education, training, and awareness programs must contain three types of activities: initial orientation; more advanced awareness, education and training commensurate with specific duties and responsibilities; and reinforcement activities.

(2) Training activities pursuant to the requirements of this policy must be conducted by individuals knowledgeable of INFOSEC principles, concepts, and application.

(3) Reference rr establishes the requirement for US Government departments and agencies to implement training programs for INFOSEC professionals IAW references u and v. An INFOSEC professional is an individual responsible for the security oversight or management of national security systems during each phase of the system's life cycle.

(INTENTIONALLY BLANK)

ENCLOSURE C

RESPONSIBILITIES

1. In implementing policies outlined in reference a and this instruction, the following responsibilities are associated with defensive IO.

a. The Chairman of the Joint Chiefs of Staff, as the principal military adviser to the President, the Secretary of Defense, and National Security Council, is responsible for developing and providing US military policy, positions, and strategy supporting DOD defensive IO. To assist the Chairman, the designated Joint Staff directorate head will ensure the following:

(1) The Director for Intelligence, Defense Intelligence Agency (DIA) (J-2), in addition to responsibilities in reference a, will:

(a) Develop joint intelligence doctrine and policy for defensive IO in coordination with DIA, NSA, and the military intelligence community.

(b) Ensure unified commands and the Joint Staff receive direct intelligence, counterintelligence, and counterdeception support to assist planning and execution of defensive IO actions across the range of military operations.

(c) Coordinate with the unified commands, DISA, NSA, DIA, and the Joint Staff to develop effective methods for identifying potential IO threats, identifying indications of threat activity, and disseminating warnings of assessed activities.

(2) The Director for Operations (J-3), in addition to responsibilities in reference a, will:

(a) Coordinate with the Director for Command, Control, Communications, and Computer Systems (J-6) for IA and appropriate defensive IO elements which support operations.

(b) Act as the focal point on the Joint Staff for all operational matters pertaining to IO such as coordinating the unified commands' military response to an IO attack and responding to time-sensitive requirements of the CINCs.

(c) Coordinate the efforts of Joint Staff elements and Defense agencies to develop and integrate into the planning process such defensive IO capabilities as counterintelligence, counterpsychological operations, and counterdeception.

(d) Develop procedures for assessing and responding to IO attacks reported to the National Military Command Center (NMCC). Procedures should include assessing the impact of such reported attacks on current or planned operations, establishing appropriate reporting and notification procedures within the Joint Staff, and developing and coordinating appropriate response.

(3) The Director for Command, Control, Communications, and Computer Systems (J-6), in addition to responsibilities in reference a, will:

(a) Coordinate with the Director, Operational Plans and Interoperability (J-7), to ensure IA and associated defensive IO capability integration into deliberate and crisis planning in a manner consistent with joint policy and doctrine.

(b) Develop IA and associated defensive IO doctrinal concepts for integration into joint doctrine in coordination with the Director J3. Ensure this doctrinal effort addresses a process that integrates the various disciplines and capabilities associated with protecting and defending information and information systems.

(c) Coordinate with Services, Defense agencies, and the Joint Staff to validate combatant command requests to release COMSEC equipment to foreign governments and international organizations.

(d) Establish and chair an IA panel, reporting to the Military Communications-Electronics Board, to review interoperability issues related to security architecture and standards for defense information infrastructure (DII) protection.

(e) Coordinate with the Director, Operational Plans and Interoperability (J-7), to ensure IA is properly exercised in CJCS coordinated and directed exercises and command exercises.

b. The combatant commanders, in addition to responsibilities in reference a, will:

(1) Develop and implement a command information defense education, training, and awareness program.

(2) Develop a process within the CINC and JTF staffs to effectively integrate the various disciplines and capabilities associated with protecting and defending information and information systems.

(3) Integrate defensive IO procedures, processes, and capabilities into daily operations and joint exercises and wargames.

(4) Identify requirements for information system interoperability (and required security services) with allies and submit to the CJCS appropriate requests to release protection technologies.

(5) Provide representation to appropriate joint and agency defensive IO working groups.

(6) Develop, coordinate, and execute military response to IO attacks.

c. The Commander in Chief, US Space Command, in addition to the responsibilities in para 1b and reference a, will coordinate with the civilian space communications community on all COMSEC matters.

d. The Service Chiefs, in addition to responsibilities in reference a, will:

(1) Integrate defensive IO concepts into Service doctrine.

(2) Exercise defensive IO capabilities in realistic scenarios.

(3) Conduct vulnerability analysis of Service components of DII to assist in assessing the vulnerabilities of defense information systems and maintain procedures and capabilities to mitigate assessed vulnerabilities and threat effects.

(4) Develop and integrate information system incident reporting program as a component of DOD-wide process.

(5) Conduct INFOSEC monitoring operations as appropriate, subject to the provisions of law, Executive orders, applicable Presidential directives, and this instruction, including:

(a) Develop procedures for conducting COMSEC monitoring consistent with the policy and procedures at Enclosure D. The Attorney General must approve the procedures.

(b) Establish procedures for notifying personnel and appropriate contractors of the COMSEC monitoring policies established in reference s.

(c) Biennially provide the Director, National Security Agency, a list of those organizations that notified personnel and contractors of the provisions of this instruction.

(6) Ensure all military and civilian personnel receive appropriate education and training to include:

(a) Annual certification training for users that addresses information systems vulnerabilities; basic capabilities and procedures for protecting information and preventing systems intrusions; and procedures for reporting actual or suspected intrusions or incidents to systems administrators or designated representatives. See Appendix H to Enclosure D.

(b) Initial and periodic training for system/network administrators that follows guidelines and standards established by the National Security Agency and the Defense Information Systems Agency (see section 1e 8).

e. The Director, National Security Agency (DIRNSA), in addition to responsibilities in reference a, will:

(1) Oversee administration of the National Security Information Systems Incident Program (NSISIP), including the items listed below. Coordinate with DISA and DIA to integrate these efforts with those to protect the DII.

(a) Oversee National Security Incident Response Center (NSIRC) administration and ensure coordinated responses to security incidents and vulnerabilities threatening national security systems.

(b) Develop, review, and revise procedures and guidance for the NSISIP.

(c) Facilitate cooperation and coordination between organizations (such as DISA and the Services) responsible for reacting to information systems security incidents.

(d) Coordinate with DIA for all-source threat analysis.

(e) Conduct vulnerability analysis of national security systems.

(f) Facilitate and coordinate identification and development of appropriate countermeasures.

(g) Facilitate development and use of specialized technical tools.

(h) Supplement other DOD activities with timely, effective support during security incidents.

(i) Facilitate security incident reporting involving legal violations to the appropriate authority.

(j) Review all reported national security systems vulnerabilities and incidents and evaluate the need for and extent of follow-up actions.

(k) Develop and disseminate NSISIP reports required at the national level.

(l) Assist in coordinating national level response to attacks against national security systems.

(2) Develop and promulgate technical criteria, standards, and guidelines for certification of national security systems.

(3) Regarding protection of telecommunications systems handling unclassified national security-related information:

(a) Provide consultation and guidance for use in determining exploitation risk.

(b) Prescribe cryptographic equipment and techniques to be used where there is a significant exploitation risk.

(c) Provide information for use of commercial cryptographic equipment and techniques where there is not a significant exploitation risk.

(4) Regarding control of compromising emanations:

(a) Apply TEMPEST suppression techniques and protective measures to cryptographic equipment and certify the TEMPEST acceptability of cryptographic equipment.

(b) Operate a National TEMPEST Information Center, which provides for a continuing exchange of TEMPEST information among US Government organizations.

(c) Encourage US industry to voluntarily develop and offer equipment and systems designed to satisfy US Government TEMPEST standards.

(d) Fund, establish, and manage a training program required for both the technical education of TEMPEST personnel and the specific training of CTTAs.

(e) Publish an annual assessment of the domestic and foreign TEMPEST threat based on all-source intelligence data.

(f) Provide guidance to departments and agencies on the security classification and control of information pertaining to compromising emanations, to include the releasability of such information to US Government contractors and to foreign nations.

(5) Regarding release of COMSEC information to allies, US contractors, and other US nongovernmental sources:

(a) Maintain a consolidated record of COMSEC contract and release notices.

(b) Approve waivers from established physical security standards for protecting COMSEC information and material.

(6) Regarding use of cryptosystems in high risk environments:

(a) Coordinate with other US Government departments and agencies to establish criteria for identifying high risk environments for cryptosystems.

(b) Establish and publish criteria for selecting cryptosystems for use in high risk environments.

(c) Maintain oversight regarding cryptosystem selection for use in a high risk environment.

(7) Regarding INFOSEC monitoring:

(a) Advise and assist other DOD components in establishing their operating procedures to implement COMSEC monitoring activities.

(b) Conduct monitoring of government telecommunications IAW reference v and Enclosure D.

(8) Regarding INFOSEC education, training, and awareness, collaborate with the Defense Information Systems Agency (DISA)/INFOSEC Program Management Office (IPMO) to:

(a) Develop INFOSEC education, training, and awareness program guidelines, including minimum training standards for users and system/network administrators, for use by other DOD components.

(b) Assist other DOD components in developing and/or conducting INFOSEC training activities.

(c) Develop appropriate INFOSEC training courses.

f. The Director, Defense Intelligence Agency, in addition to responsibilities in reference a, will:

(1) Provide direct intelligence assistance to the combatant commands in the planning and execution of defensive IO activities.

(2) Conduct analysis of IO threat information.

(3) Provide precise and timely intelligence for threat identification to the combatant commands, DISA, NSA, and the Joint Staff.

(4) Support Joint Staff, combatant commands, and Service efforts to ensure integrated tactical, operational, and strategic military requirements are developed and communicated to the intelligence community.

(5) Serve as the DOD focal point for intelligence support to the indications and warning process (I&W).

g. The Director, Defense Information Systems Agency, in addition to responsibilities in reference a, will:

(1) As the DOD single point of contact for information technology standard development (information, information processing, and information transfer) (reference rr), establish a security architecture and standards for protecting and defending the DII. The installation premise router will serve as the demarcation point between the public switched network and defense information system network.

CINCs, Services, and defense agencies should share information with DISA relative to protection of the DII. DISA will collaborate with DIA and NSA, as appropriate.

(2) Develop an information system incident program and a SIRC for protection and defense of the DII. Coordinate with NSA to ensure integration of this program and SIRC with NSA's NSISIP and NSIRC. At a minimum, the program should include:

(a) Establishing and operating a SIRC to centrally coordinate actions involving DII security incidents and vulnerabilities.

(b) Developing, reviewing, and revising IA procedures and guidance for the program.

(c) Facilitating cooperation with organizations (such as the Federal Bureau of Investigation) that handle information systems incident responses occurring outside the DII.

(d) Coordinating with DIA for all source threat analysis.

(e) Conducting vulnerability analyses of the DII backbone.

(f) Facilitating and coordinating (in collaboration with NSA) identification and/or development of appropriate countermeasures.

(g) Facilitating (in collaboration with NSA) development and use of specialized technical tools.

(h) Providing effective and timely security incident response support to other DOD activities.

(i) Developing, within six months after implementation of this instruction, DII incident reporting policy and procedures to include thresholds for incident reporting (suspected or actual probes, intrusions, or attacks) across the CINCs Services, and Defense Agencies. Policy and procedures should also include coordination and assessment with appropriate intelligence and law enforcement agencies, notification to the National Military Command Center, and report-back mechanisms to ensure appropriate actions were initiated.

(j) Establishing, in coordination with the NSA, DIA, and appropriate law enforcement agencies, a database of all reported incidents.

(k) Submitting weekly reports to the Joint Staff summarizing the nature and status of reported incidents.

(3) Ensure the DII contains adequate protection against attack.

(4) Provide technology and services to ensure the availability, reliability, maintainability, integrity, and security of the DII in consultation with DIA and NSA.

(5) Assist in assessing the vulnerabilities of defense information systems and maintain procedures and capabilities to mitigate assessed vulnerabilities and threat effects.

(6) Regarding INFOSEC education, training, and awareness. Through the IPMO:

(a) Develop INFOSEC education, training, and awareness program guidelines, including minimum training standards for users and system/network administrators, for use by other DOD components.

(b) Assist other DOD components in developing and/or conducting INFOSEC training activities.

(c) Integrate appropriate INFOSEC/IA training courses.

h. The Commander, Joint Communications Support Element (JCSE), will ensure appropriate protection for telecommunications and information systems services provided IAW reference ss.

i. The Director, Joint Command and Control Warfare Center (JC2WC), will:

(1) Coordinate with the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6), for IA, appropriate defensive IO and C2 protection elements, and mission needs statements interoperability certification.

(2) Coordinate C2 vulnerability analyses with the J-6.

j. All DOD components will:

(1) When planning for the protection of telecommunications and information systems (including AISs):

(a) Determine the exploitation risk to national security-related information in consultation with DIRNSA. Coordinate with DIRNSA on communications protection where there is a significant risk of telecommunications exploitation.

(b) Where appropriate, use only NSA-approved equipment and techniques, and NSA-produced or NSA-approved keying material to satisfy classified information protection requirements.

(c) Decide what unclassified information intended for transmission is related to national security and protect accordingly (see Enclosure B).

(2) With regard to the control of compromising emanations:

(a) Implement and manage a single compromising emanations control program for national security systems. The program should include provisions for:

1. Evaluating equipment, systems, and facilities to determine the need for TEMPEST countermeasures and for conducting periodic on-site evaluations of the effectiveness of those countermeasures.

2. Appointing CTTAs in accordance with NSTISSC-approved criteria to ensure TEMPEST countermeasures incorporated at facilities and in equipment/system development programs are consistent with applicable national policy and specific NSTISS instructions. A CTTA from one DOD component may provide this service to another DOD component.

(b) Provide annually to the TEMPEST Advisory Group (TAG) the name(s) of component CTTAs for the distribution of technical TEMPEST countermeasures information.

(c) Submit promptly to DIRNSA any information related to the TEMPEST threat.

(d) Ensure that CTTAs:

1. Conduct or validate all TEMPEST countermeasure reviews required by NSTISS issuances.

2. Maintain a record of all TEMPEST countermeasure reviews conducted, recommendations provided, and estimated cost of implementation.

3. Coordinate with CTTAs of other US Government departments or agencies when countermeasures for shared facilities are being considered.

(3) Ensure that a designated approving authority (DAA) is identified for each national security system under their operational control and that DAAs have the ability to influence the application of resources to achieve acceptable security.

(4) Establish access controls for classified cryptographic information (see Glossary) and apply these access controls to all individuals satisfying criteria in Enclosure D, whose official duties require continuing access to classified cryptographic information, including:

(a) Developing and administering a "Cryptographic Access Briefing" addressing the specific security concerns of the DOD component. An example briefing is presented in Enclosure D.

(b) Cryptographic access certification including a certificate signed by all individuals granted cryptographic access.

(c) Ensuring applicable security directives contain requirements for reporting unofficial foreign travel and contacts with foreign nationals.

(d) A capability to administer required polygraph examinations. This may be accomplished either by directly programming and funding for these resources or by executing agreements and arrangements to use the existing resources of another DOD component.

(5) Ensure that the policy requirements for releasing COMSEC information outside the government are met (Enclosure D).

(6) When planning for employment of cryptosystems in high risk environments:

(a) Identify specific high risk locations where cryptosystems may be deployed in accordance with standardized criteria, and notify DIRNSA of all such designations.

(b) Apply the criteria published by DIRNSA in selecting cryptosystems for use in high risk environments, and notify DIRNSA of their selection.

(c) Select, procure, install, operate, and maintain cryptosystems selected for use in high risk environments.

(d) Ensure that only minimum amounts of mission essential COMSEC materials are placed in high risk environments.

(e) Ensure that effective and workable plans, and adequate manpower and materials are available to protect, evacuate, or destroy COMSEC materials in high risk locations which are jeopardized.

(f) Notify appropriate COMSEC authorities when cryptosystems used in high risk environments are destroyed, lost, damaged, captured, or compromised.

(g) Make reasonable efforts to return abandoned equipment and COMSEC materials to proper control.

(7) Plan, program, fund, implement, and manage those electronic keying programs necessary to meet the national policy objective eliminating dependence on paper-based/nonelectronic keying methods by the year 2000.

(8) Establish a SIRC for information system defense, including meeting the objectives of the NSISIP program, and:

(a) Identify to the NSISIP program administrator an individual to act as their organization's focal point for this program.

(b) Ensure direct reporting of violations of law or information attacks to the appropriate authority. As a minimum, all incidents (known or suspected probes or intrusions) should be reported to the appropriate Computer Emergency Response Team for subsequent evaluation and reporting to DISA and, if necessary, the National Military Command Center.

(c) Develop organizational policies, procedures, and guidance to defend information systems, including implementing the NSISIP program.

(9) Regarding INFOSEC education, training, and awareness:

(a) Develop, implement, and evaluate INFOSEC education, training, and awareness programs in accordance with NSA and other applicable guidelines.

(b) Consistent with applicable laws, security requirements, policies, and resource availability, make information copies of INFOSEC education, training, and awareness materials available to NSA and DISA/IPMO.

(INTENTIONALLY BLANK)

ENCLOSURE D

PROCEDURES

1. This enclosure contains procedural guidance for implementing defensive IO. Procedures are outlined in the following appendixes:

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE D

AUTOMATED INFORMATION SYSTEM SAFEGUARDS

1. General. Continuously employed safeguards ensure AIS resource protection against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Safeguards include administrative, procedural, personnel, physical, environmental, and technical measures, and education and training as required.

2. Scope. The scope of this appendix is AISs as defined in the Glossary. AISs vary widely, some designed for C2, some imbedded in weapons systems, and some designed for controlling infrastructure components. For example:

a. While the term information systems include C2 systems, the term AISs does not include all C2 systems. A point-to-point radio link is an information system, and may also be a C2 system, but not necessarily an AIS.

b. Similarly, the term C2 systems does not include all information systems or AISs. For example, an intelligence radio net is an information system, but not necessarily a C2 system. Similarly, a medical logistics AIS is an information system, but not considered a C2 system.

3. Safeguards. The mix of safeguards selected for an AIS processing classified or sensitive unclassified information will ensure the AIS meets minimum requirements as set forth in Annex A to this appendix. Minimum requirements will be met through automated and manual means in a cost-effective, integrated manner.

4. Life Cycle Security Policy. Security policy will be considered throughout the life cycle of an AIS, from concept development through disposal. A Designated Approving Authority (DAA) will be designated as responsible for the overall security of the AIS. The following conditions will be met:

a. The AIS developer is responsible for ensuring early and continuous involvement of users, information system security officers, data owners, and DAA(s) in defining and implementing AIS security requirements. There will be an evaluation plan for the AIS showing progress towards full compliance with stated security requirements.

b. Mandatory safeguard requirement statements will be included, as applicable, in the acquisition and procurement specifications for AISs. The statements will be the result of an initial risk assessment and will specify the level of trust required under reference uu.

c. No classified or sensitive unclassified data will be introduced into an AIS without designation Data entry approval will be obtained from the data owner where applicable.

d. Accreditation of an AIS will be supported by: a DAA-approved certification plan in compliance with the DOD Information Technology Security Certification and Accreditation Process; risk analysis of the AIS in its operational environment; security safeguard evaluation; and a certification report. Accreditation of computers embedded in a system may be at the system level.

e. A program for periodically reviewing safeguard adequacy for operational, accredited AISs will be established. To the extent possible, persons independent of the user organization and the AIS operation or facility will conduct reviews.

f. AISs will include a capability (automated to the extent possible) to enable users and administrators to identify attempts to breach system security.

g. A program for developing and testing contingency plans will be established. The contingency planning objective is to provide reasonable AIS continuity support during unusual operations. Plans should be tested periodically under realistic operational conditions.

h. Changes affecting AIS security must be anticipated. Changes to the AIS or associated environment affecting safeguards or resulting in changes to the prescribed security requirements will require reaccreditation. This provision includes each permanent connection to other AISs and permissions to establish temporary connections with other AISs (see paragraph 5 below). Reaccreditation will take place before the revised system is declared operational.

i. A program for disposing of AIS components will be established. An AIS disposal program must ensure that all damaged, destroyed, obsolete, or excess AIS hardware or software components are properly accounted for and handled in a manner that is consistent with security policy.

5. Memoranda of Agreement for Interfacing Networks.

a. A memorandum of agreement (MOA) is required addressing the accreditation requirements for each AIS when interfacing or networking AISs managed by different DAAs.

b. The MOA should include:

(1) Description and classification of the data and the AISs.

(2) User clearance levels.

(3) Designation of the DAA resolving conflicts.

(4) Safeguards to be implemented before interfacing the AISs.

c. MOAs are required when:

(1) A DOD AIS interfaces with a contractor AIS, another DOD AIS, or other government (non-DOD) AIS.

(2) A contractor's AIS interfaces with another contractor's AIS.

d. For a multiuser telecommunications network (e.g., the Defense Information System Network (DISN) or the Global Command and Control System (GCCS)), a DAA will be designated as responsible for overall network security and determine security and protection requirements for AIS connection to the network.

e. Necessary safeguards will be implemented and the AISs accredited before they are connected to the network.

f. The security of each AIS connected to the network remains the responsibility of its DAA.

g. The DAA responsible for overall network security will have authority and responsibility to remove any AIS not adhering to network security requirements.

h. Where needed, it is permissible to define network interfaces and boundaries into manageable subnetworks based on physical or logical boundaries. Cryptographic separation and/or equivalent COMPUSEC measures, as defined by the NSA, DISA, or DIA, will be a basis for defining such network interfaces or boundaries.

i. While the DAAs of the subnetworks retain responsibility for their network security, the overall network DAA is responsible for network interface security as part of the responsibility for the overall network.

j. Networks, including connected subnetworks, will be accredited for the highest division and class of security required based on the concepts and procedures in Annex B to this appendix.

k. DAAs will ensure that networks are not connected to other networks without first gaining DAA concurrence of networks already connected.

6. Foreign Access. Access by foreign nationals to a DOD-owned or DOD-managed AIS may be authorized only by the DOD component head and will be consistent with DOD, the Department of State (DOS), and the Director of Central Intelligence (DCI) policies.

7. Movement of Information from SCI to non-SCI Environment. An AIS accredited to process and/or store Sensitive Compartmented Information (SCI) may use NSA approved automated means (software, firmware, or hardware) to permit classified non-SCI data to be extracted from the SCI system. This capability is permissible only if it was considered and approved as part of the security accreditation and the AIS is operating at a minimum security class of B1 described in reference uu.

ANNEX A TO APPENDIX A TO ENCLOSURE D

MINIMUM SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS

1. Minimum Security Requirements. Cost-effective integration of automated or manual means will meet the following minimum requirements (reference bb):

a. Accountability. Each person having AIS access may be held accountable for his or her actions on the AIS. An audit trail will provide a documented history of AIS use. Sufficient detail in the audit trail will allow event reconstruction to determine cause or magnitude of compromise should a security violation or malfunction occur. Automated audit capabilities will, to the extent possible, include an automated capability (an “alarm” system) to alert system administrators of attacks on the system.

(1) The audit trail will be in continuous operation to document the following:

(a) Identity of each person and device having AIS access.

(b) Time of the access.

(c) User activity sufficient to ensure user actions are controlled and open to scrutiny.

(d) Activities that might modify, bypass, or negate safeguards controlled by the AIS.

(e) Security-relevant actions associated with processing periods or the changing information security levels.

(2) DAAs determine the retention period for the audit information for their systems. DAAs also determine audit trail requirements for stand-alone, single-user AIS (e.g., personal computer (PC), memory typewriter, drafting machine). Similarly, DAA determines requirements to include an automated “alarm” capability to alert system administrators to attacks and real time audit readout capability. Larger systems with advanced audit capability will require audit reduction tools. If an automated “alarm” capability is needed but not available, a DAA may approve interim authority to operate, with appropriate manual review of audit records, until a suitable alarm is installed.

b. Access. Each AIS will have access control policy. The policy will include features and/or procedures enforcing access control policy. User identity will be positively established before authorizing access.

c. Security Training and Awareness. A security training and awareness program will be in place for all persons accessing the AIS. The program will ensure all persons responsible for the AIS and information are aware of proper operational and security-related procedures and risks.

d. Physical Controls. AIS hardware, software, and documentation, and all classified and sensitive unclassified data handled by the AIS will be protected to prevent unauthorized disclosure, destruction, or modification (i.e., data integrity will be maintained). Control and protection levels will be commensurate with the maximum sensitivity/value of the information. This includes personnel, physical, administrative, and configuration controls. Additionally, protection against AIS resource denial (e.g., hardware, software, firmware, and information) will be consistent with the information sensitivity. Software development and related activities (e.g., systems analysis) will be protected when it is determined that the software will be used for handling classified or sensitive unclassified data.

e. Least Privilege. The AIS will allow each user access to authorized information and functions only.

f. Data Continuity. Each AIS file or data collection will have an identifiable source. Its accessibility, maintenance, movement, and disposition will be governed by security clearance, formal access approval, and need-to-know.

g. Data Integrity. There will be safeguards in place to detect and minimize inadvertent modification or destruction of data.

h. Contingency Planning. Contingency plans will be developed and tested in accordance with reference b to ensure AIS security controls function reliably or, in the event of their failure, that adequate backup functions are in place.

i. Accreditation. Each AIS will be accredited to operate in accordance with DAA-approved safeguards.

2. Risk Management. There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical way of providing needed protection.

ANNEX B TO APPENDIX A TO ENCLOSURE D

NETWORK CONSIDERATIONS

1. For purposes of accreditation, a network will be treated as either a connection of accredited AISs (which may be networks) or as a unified network (reference bb). These two cases are discussed below:

a. Case 1 - Interconnections of Accredited AISs

(1) If a network consists of previously accredited AISs, an MOA is required between each component AIS DAA and the network DAA. The network DAA must ensure interface restrictions and limitations are observed for connections between AISs. Reference vv provides applicable interface restrictions and limitations. In particular, connections between accredited AISs must be consistent with AIS operation, sensitivity level or range of sensitivity levels for which each AIS is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.

(2) Each AIS will be assigned an accreditation range consisting of the security levels associated with data sent over the network connection. If the accreditation range is more than a single level, the AIS must reliably segregate data by level, and accurately label it for multilevel transmission.

(3) DOD component AIS DAAs should be aware that connection to a network involves additional risk because of the data exposure to the larger network. In connections to adjacent AISs, operational modes and security mechanisms of those AISs should be taken into consideration. Simple accreditation of a system may not meet a particular component's security requirements.

(4) Untrusted and unaccredited AISs may be components of a network. Connections between them and other component AISs are permissible under the same conditions in subparagraph 1a(1), above. Only unclassified information, not to include sensitive unclassified information, may be sent to and from unaccredited AISs.

(5) Special support AISs, such as packet switching nodes and terminal access interfaces, must be individually accredited if they carry classified or sensitive unclassified information. The network DAA serves as the DAA for all such AISs.

b. Case 2 - Unified Networks

(1) Some networks may be wholly accredited without prior accreditation of each of their components. It is necessary to treat a network as unified when some of its component AISs are so specialized or dependent on other components of the network for security support that individual accreditation is not possible or meaningful with respect to secure network operation. In order to be accredited, a unified network will possess a coherent network security architecture and design, and should be developed with an attention to appropriate security requirements, mechanisms, and assurances.

(2) The recommended approach for accrediting a unified network is to apply the risk management procedures (enclosure to reference bb) to the entire network and subsequently determine an evaluation class. Requirements to meet that evaluation class are obtained from an applicable interpretation of reference uu.

ANNEX C TO APPENDIX A TO ENCLOSURE D

CONTROLLED ACCESS PROTECTION

1. General. All AISs accessed by more than one user, when those users do not have the same levels of access, will be assessed and certified to the degree they provide automated Controlled Access Protection for classified and sensitive unclassified information (reference p).

2. Controlled Access Protection. A technical description of Controlled Access Protection is found in reference uu. Major characteristics include:

a. Individual accountability through identification and authentication of each individual AIS.

b. Audit trail maintenance of security-relevant events.

c. An ability to control information access according to user authorization.

d. Preventing one user from obtaining another user's residual data.

3. Exceptions. A risk management approach will be employed in granting exceptions to Controlled Access Protection policies by DAAs.

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE D

PROTECTION OF UNCLASSIFIED NATIONAL SECURITY INFORMATION AND SENSITIVE INFORMATION

1. Reference h and ww require all sensitive (national security-related) information to be protected commensurate with associated exploitation risks. Department and agency heads are responsible for deciding which of their transmittable unclassified information is sensitive (national security related). This appendix provides guidelines for identifying telecommunications containing unclassified national security-related information in this category.

2. Information drain to our adversaries through exploitation of the nation's unprotected telecommunications systems poses a serious threat to our national security. The need to protect telecommunications requires participation among DOD, government, and the private sector. Telecommunications systems between government agencies and their contractors, between government contractors, or between government contractors and their subcontractors must be protected. Whenever telecommunications have value and can be intercepted, it should be expected that attempts will be made to exploit them. Generally, if the government department, agency, contractor, or subcontractors believe the information will be useful to an adversary, it should be protected.

3. These guidelines pertain only while information is being electrically transmitted. If this information is not protected during transmission, it is vulnerable to interception and exploitation. Attached guidelines (Annex A to this appendix) identify kinds of information for which intercept would be contrary to the national interest.

4. Annex A is a guideline only. Omission of a particular information category or type does not preclude a separate determination that such information is valuable to an adversary. Departments and agencies are encouraged to establish additional guidelines to suit their particular needs.

5. The guidelines provide a sample of specific categories and types of information considered to be sensitive (national security-related). Relative values of each information type are on a six point scale, with "1" being the highest. These values generally describe expected benefits of protection and a suggested priority for safeguarding this information.

Information types with assigned values of 1, 2, or 3 should be presumed to require protection whenever an exploitation risk is present. Values 4, 5, or 6 may also require protection when an exploitation risk is present, depending on the timeliness of the information, its quantity, or other characteristics. A case-by-case evaluation may be appropriate in such circumstances.

ANNEX TO APPENDIX B TO ENCLOSURE D

GUIDELINES FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS

INFORMATION VALUE GUIDE

VALUE CATEGORY

1. Military

1 a. Force Planning. Doctrine, concepts, and plans for employing strategic and general purpose forces; national strategic targeting philosophies and doctrine for the nuclear weapon employment, stockpile maintenance; national appraisal of opposing capabilities and vulnerabilities; national C2 systems, their strengths and vulnerabilities; military production and procurement, level and composition of military expenditures, including changes in funding levels for the military sector for major components of military spending, military RDT&E expenditures.

1 b. Strategic Offensive Forces. Nonspecific capabilities of the ICBM force, ballistic and cruise missile submarine forces, long-range ballistic missile forces, strategic doctrine, general capabilities for use of space vehicles in a nuclear offensive role; and general characteristics of strategic offensive weapons systems.

1 c. Strategic Defense Forces. Nonspecific capabilities of the ballistic missile defense force, fighter/interceptor defense force, surface-to-air missile force, antisubmarine warfare forces, strategic doctrine, intelligence collection systems, equipment, and facilities; general capabilities for attack against space satellites; nuclear explosion assessment system; RDT&E on strategic defense weapon systems; and R&D related to development of beam weapons.

2 d. Armed Conflict, Hostilities Indications and Warning. Indications of preparation for or initiation of an attack.

2 e. General Purpose Forces. Capabilities and vulnerabilities of ground forces, naval forces, air transport forces, and tactical air forces, including strength, organization disposition, C2, tactical doctrine, operating practices, training levels, mobility, support systems availability, equipment and facilities; biological and chemical warfare doctrine and concepts; capabilities and vulnerabilities of paramilitary forces such as border guards, national policy forces, and internal security forces, RDT&E on and characteristics of general purpose systems.

2 f. Support Capabilities and Military Environment. General capabilities of Service components to render services required by military forces to execute assigned missions; influence of country's physical environment on capabilities, dispositions or mobility of military forces; existence of plans and programs to limit casualties and damage to countervalue targets by civil defense or other passive means, general capabilities to support military forces in combat, training and readiness of reserve forces, mobilization system and time-phased capabilities of the mobilization program; concepts, doctrine, strategy, and tactics and capabilities for using electronic warfare; RDT&E on and characteristics of military electronics systems.

3 g. Arms Transfer, Military Assistance, and Out-of-Country Deployments. Provision of arms and military assistance, acceptance of arms and military assistance, including transfers, negotiations/contracts, sales/loans/grants, and deliveries of military and military-related equipment, services, and/or military training; national plans, capabilities, and actions to deploy forces and associated weapons to foreign countries, in international waters, in airspace or outer space, including the purposes and priority attached to deployment to particular countries or areas.

2. Political

1 a. Attitudes and Actions toward Arms Control, Force Limitations, Cease-Fire and/or Peace Agreements. National attitudes, actions, and compliance concerning arms limitations proposals; political military assessment of related risks and limitations of arms control, force level agreements, cease-fire or peace treaties; policy objectives and actions regarding strategic and regional arms control and disarmament.

2 b. Intelligence and Security Services. Effort to deceive, neutralize, or interfere with foreign target technical intelligence collection capabilities; structure, capabilities, and effectiveness of positive intelligence and CI organizations internal security effectiveness; subversion techniques; national capabilities to conduct psychological warfare operations; capabilities and programs for sabotage directed against personnel, programs and facilities of other nations.

2 c. US National Security Objectives. National objectives for development of a security posture vis-à-vis potentially hostile nations; policies, intentions, programs and actions favoring or inhibiting active participation in military alignments or alliances, including the receipt and/or provision of military support.

2 d. US Foreign Relations with Developing Countries. National foreign policy intentions, objectives, programs, negotiating positions, and actions.

3 e. US Foreign Relations with Allies. National foreign policy intentions, objectives, negotiating positions, and actions.

3 f. US Participation in Multilateral Organizations. National policy objectives, programs, negotiating positions, and actions likely to support or conflict with political and economic interests of other nations as they relate to the functioning and activities of international organizations of all types (e.g., the United Nations and its organizations) except military alliances.

4 g. Resource and Environmental Issues. National interest in and actions to deal with environmental problems, especially atmospheric and water pollution; to regulate exploitation of polar, ocean, and sea bed resources; and to promote favorable action on law of the sea issues.

4 h. Internal Political Affairs. Domestic policy objectives, programs, and actions; internal political developments; changes in the representation and roles of politically significant parties and factions; key influences, on the internal decision making process; government capability to identify and deter/suppress elements fostering insurgency.

4 i. US Political Biographic Data. Background, associations, actions, medical and psychological data on key political figures. Personality data on key figures to include leadership style, decision making, attitudes, world view, crisis reaction, and negotiating behavior.

5 j. Transit Rights, Authorizations, and Facilities Arrangements. National attitudes and actions regarding the granting of transit rights, authorizations, and facilities arrangements.

3. Economic

2 a. Technology Transfer. Attitudes and policies toward technology transfer; compliance with international strategic trade controls.

3 b. Energy Resources and Policies. Capacity to produce and access to oil, coal, nuclear and other energy resources; plans and policies for exploitation and marketing, conservation and control of use; stockpiling, export and import; policies on pricing and participation in multilateral efforts affecting supply, including forecasts of energy demand.

3 c. Telecommunication Services. The capabilities and location of civilian and military telecommunications equipment and facilities, including landline (wire and cable), radio (troposcatter, radio relay and satellite systems), telephone, teleprinter, facsimile, data transmission, television, and other services.

3 d. Agricultural Policies, Food Supplies and Mineral Resources. Capacity to produce and access to food and foodstuffs; impact on population of marketing, stockpiling and control of food products and fisheries; capacity to produce and access to minerals and mineral products; plans, policies and activities affecting access to resources, including producers consumer marketing arrangements.

4 e. Monetary and Financial Developments. Fiscal and monetary policies and objectives; national budgets and financing of national debt; balance-of-payment objectives, including exchange rate policy; gold prices and transactions; international monetary proposals.

4 f. Business Activities and Conditions. Commercial and financial developments; business conditions, sales opportunities for US manufacturers and industrial products; sales opportunities for investment and investment climate; investment activities at home and abroad; government procurement activities, and changes in trading policies that affect export opportunities for US producers.

4 g. Activities of Multinational Corporations. Activities of foreign multinational corporations as they affect economic relations between the US and subject country, including specific inward and outward foreign investment deals; technology transfer; the amount of production, foreign trade, and sales attributable to foreign subsidiaries of US firms.

4 h. Foreign Economic Relations with Advanced Countries. Foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.

4 i. Foreign Economic Relations with Other Countries. Foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.

5 j. Economic Growth and Stability. Changes in leading economic indicators; economic policy responses to such internal and external changes in economic performance, the likely effects of these responses.

5 k. Industrial Production. Capacity to produce basic, intermediate, and final industrial goods needed for civilian and military use; prospective evolution of the industrial sector.

5 l. International Trade Trends. Value, tonnage, and commodity composition of exports and imports, especially changes in market shares; disparities between export and domestic prices of export goods, transportation bottlenecks in foreign trade.

5 m. Trade and Transport Policies and Negotiating Positions. Trade liberalization, tariff and nontariff barriers other restrictions, proposed commodity agreements, export credit policies and policies regarding trade in major crops; plans and policies related to commercial air or maritime activities.

5 n. Advanced Industrial and Manufacturing Processes and Products. New investment and application of funds (including extent of government subsidy) and other resources to the research, development, testing, and application of new, advanced industrial and manufacturing processes and products, and the introduction or manufacture of significant new products.

5 o. Foreign Economic Relations with Communist Countries. Foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.

5 p. Transportation Systems. The operational capabilities, vulnerabilities, and limitations of transportation networks and facilities (railways, highways, airlines, waterways, pipelines, transshipment areas, warehouses, airfields, ports and harbors), to include their use by military forces for movement of supplies and reinforcements; capabilities, disposition, and employment of merchant fleet.

4. Special Subjects

1 a. Other Government Information. Information provided to the US by a foreign government or international organization, or produced by the US under an arrangement with such entity, with expectation or condition that the information will be private.

b. Other Agency Information. Information provided to DOD by another US department or agency with the expectation or condition that the information will be protected within DOD.

c. Technology. Any design, manufacturing, and related technical data concerning critical arrays of know-how identified on the DOD Military Critical Technologies List.

d. Weapons of Mass Destruction (WMD). WMD proliferation including nuclear, chemical, and biological devices, infrastructure, C2 systems, delivery systems, acquisition programs, the decision by nation states, sub-national groups or terrorist organizations to pursue WMD technology including research and development facilities, special nuclear materials, precursor chemicals, actions of source countries or organizations. Transportation and safeguards.

e. National Science Policies and Programs. The administration of and organization of science and technology work in the governmental, industrial, and academic sectors.

f. Human Rights. Attitudes and actions toward human rights.

g. Illicit Drug Traffic. Cultivation, production, processing, storage, transportation, and distribution of illicit narcotics and dangerous drugs; related economic and financial transactions, including money laundering and recycling; activities of non-governmental organizations, including criminal enterprises and groups, engaged in these activities.

(INTENTIONALLY BLANK)

APPENDIX C TO ENCLOSURE D

CRYPTOGRAPHIC ACCESS CRITERIA

1. An individual may be granted access to US classified cryptographic information, only if that individual meets the following criteria (reference j):

a. Is a US citizen.

b. Is an employee of the US Government, a US Government-cleared contractor or contractor employee, or is employed as a US Government representative (including consultants of the US Government).

c. Possesses a security clearance appropriate to the classification of the US cryptographic information to be accessed.

d. Possesses a validated need-to-know.

e. Receives a security briefing appropriate to the classified cryptographic information to be accessed.

f. Acknowledges his or her access by signing a cryptographic access certificate.

2. Where department or agency heads so direct, an individual granted access in accordance with this policy may be required to acknowledge the possibility of being subject to a non-lifestyle, CI scope polygraph examination administered in accordance with department or agency directives and applicable law.

3. All persons indoctrinated for cryptographic access may be subject to special requirements, prescribed in their respective department or agency security directives, regarding unofficial foreign travel or contacts with foreign nationals.

4. These procedures apply to all individuals satisfying the requirements of paragraph 1 and whose official duties require continuing access to US classified cryptographic information. Therefore, primary consideration should be given to those individuals assigned:

a. As COMSEC custodians or alternates.

b. As producers or developers of cryptographic keys or logic.

c. As cryptographic maintenance or installation technicians.

d. To spaces where cryptographic keying materials are generated or stored.

e. To prepare, authenticate, or decode valid or exercise nuclear control orders.

f. In secure telecommunications facilities located in fixed ground facilities or on board ships.

g. Any other responsibility with access to US classified cryptographic information which is specifically identified by the head of a department or agency.

5. Exceptions to these procedures may be approved by department or agency heads to meet exigent operational needs. Records of exceptions granted will be made available on request from the National Manager for Telecommunications and Information Systems Security.

ANNEX A TO APPENDIX C TO ENCLOSURE D

SAMPLE CRYPTOGRAPHIC ACCESS BRIEFING

1. You have been selected to perform duties requiring access to US classified cryptographic information. It is essential that you are aware of facts relevant to information protection before access is granted. You must know the reason why special safeguards are required to protect US classified cryptographic information. You must understand the directives requiring safeguards and penalties you incur for unauthorized disclosure, retention, or negligent handling of information. Failure to properly safeguard information could cause serious damage or irreparable injury to US national security.

2. US classified cryptographic information is especially sensitive because it is used to protect other classified information. Any piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. Safeguards placed on US classified cryptographic information are a necessary component of government programs to ensure our nation' s vital secrets are not compromised.

3. Because access to US classified cryptographic information is granted on a strict, need-to-know basis, you will be given access to only the cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, department or agency implementing directives covering the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

4. Especially important to the protection of US classified cryptographic information is the timely reporting of any known or suspected information compromise. If a cryptographic system is compromised, and the compromise is not reported, continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

5. NOTE: The following two paragraphs will only be included when the applicable department or agency head directs.

a. As a condition of access to US classified cryptographic information, you must acknowledge the possibility that you may be subject to a non-lifestyle, CI scope polygraph examination. This examination will be administered in accordance with the provisions of (insert appropriate department or agency directive) and applicable law. This polygraph examination will only encompass questions concerning espionage, sabotage, or questions relating to unauthorized disclosure of classified information.

b. You have the right to refuse a non-lifestyle, CI scope polygraph examination. Such refusal will not be cause for adverse action but may result in your being denied access to US classified cryptographic information. If you do not at this time wish to sign such an acknowledgment of this provision as a part of executing a cryptographic access certification, this briefing will be terminated and the briefing administrator will so annotate the cryptographic access certificate.

6. You should know that intelligence services of some foreign governments prize the acquisition of US classified cryptographic information. They will go to extreme lengths to compromise US citizens and force them to divulge cryptographic techniques and materials protecting the nation's secrets. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to coercion attempts to divulge US classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions revealing your knowledge of, or access to, US classified cryptographic information and thus avoid highlighting yourself to those seeking the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding US classified cryptographic information must be reported immediately to (insert appropriate security office).

7. In view of the risks noted above, unofficial travel to certain communist or other designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

8. Finally, you must know that, should you willfully or negligently disclose to any unauthorized persons any of the US classified cryptographic information to which you will have access, you will be subject to administrative and civil sanctions, including adverse personnel actions and criminal sanctions under the Uniform Code of Military Justice and/or the appropriate criminal laws of the US, as appropriate.

APPENDIX D TO ENCLOSURE D

DISCLOSURE OR RELEASE OF COMSEC INFORMATION TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS

1. At a minimum, requests to release COMSEC information to foreign governments and international organizations will contain the following information:

a. Identity of US or binational commands having the interoperability requirement with the foreign nation or international organization. For each requirement, the request will reference nn operational plan or concept of operations plan that explains the interoperability requirement.

b. Scope, duration, and urgency of the COMSEC capability required and a statement of how the requirement is currently being met.

c. Source of cryptographic equipment or other COMSEC material needed to fulfill the requirement. Submitting commanders will coordinate with appropriate Service and cryptographic resource managers to determine the specific equipment source and whether needed equipment will be purchased under FMS or foreign military sales of cryptographic device services (FMS-CDS).

d. Provisions providing for engineering, installation, maintenance, and logistic support.

e. Facility adequacy for storing COMSEC material by recipient.

f. Equipment installation and operation plans and how physical requirements will be met.

g. Requirements for instructional material translation, such as operating or maintenance instructions.

h. Requirement milestones and impact if milestones are not met.

2. Requests will be forwarded through combatant command channels to the Joint Staff J-6 for validation prior to submission to the NSTISSC.

(INTENTIONALLY BLANK)

APPENDIX E TO ENCLOSURE D

RELEASE OF COMSEC INFORMATION TO US CONTRACTORS AND OTHER US NONGOVERNMENTAL SOURCES

1. General. COMSEC operations will normally be conducted by the government. Military forces may obtain required COMSEC support from and provide COMSEC information and material to US nongovernmental sources within limitations (reference d).

2. Security standards and procedures applicable to COMSEC information release will be consistent with established policies. In particular:

a. Individuals granted access to COMSEC information must be US citizens. Access will be controlled on a strict need-to-know basis and granted only in conformance with procedures established for the particular type of COMSEC information involved. Release request for COMSEC information to US residents who are not US citizens will be processed as an exception to policy.

b. Contracting for design, development, modification, production, or developmental testing of cryptographic equipment requires the specific approval of the DIRNSA.

c. As a prior condition of release, COMSEC information provided to US citizens not part of the government will be controlled in a manner to prevent its further dissemination or transfer outside the government.

d. Individuals requiring access to US COMSEC information must comply with applicable cryptographic access policies.

3. COMSEC information may be released when the following criteria are met:

a. A valid need must exist for an individual or organization to:

(1) Install, maintain, or operate COMSEC equipment for the US Government.

(2) Participate in the design, planning, production, training, installation, maintenance, operation, logistic support, integration, modification, testing, or study of COMSEC material or techniques.

(3) Electrically communicate classified national security information in a cryptographically secure manner, or unclassified national security-related information by COMSEC protected means.

b. Individuals granted access to classified COMSEC information must hold a final government security clearance for the classification level involved. Clearances of facility security officers, COMSEC custodians, and alternate COMSEC custodians must be predicated on a current favorable background investigation.

c. Everyone provided access to COMSEC information must be annually briefed regarding the unique nature of COMSEC information and their responsibilities to properly safeguard and control it.

d. All individuals maintaining government COMSEC equipment must receive formal NSA-approved training on such equipment.

4. DOD components identifying a requirement to release COMSEC information are responsible for:

a. Determining that such releases are in the best interests of the government.

b. Maintaining records of all organizations and self-employed individuals provided access to government COMSEC information.

c. Notifying NSA of contract awards or other releases of COMSEC information and material; information provided should include the name of the contractor, licensee, or individual; the subject matter of the contract or provision; and the nature of the COMSEC information released.

d. Ensuring performance of their contractors or licensees meets established COMSEC standards and doctrine, including standards of security and quality;

e. Incorporating specified access criteria into contracts and other appropriate documents whenever individuals who are not employees of the government provide services.

5. Exceptions to these procedures may only be granted by the NSTISSC except for waivers to physical security standards protecting COMSEC information and material, which may be approved by DIRNSA.

Prior approval must be obtained in each case. Requests for NSTISSC approval, with justification and explanatory details, will be forwarded to the NSTISSC through the DIRNSA. The following checklist should be used as a guideline.

CHECKLIST FOR PREPARING REQUESTS FOR EXCEPTIONS TO THE PROVISIONS OF NCSC-2

1. Identify the individual and/or organization, their citizenship, their level of security clearance, and the location(s) at which COMSEC functions will be performed.

2. Identify the COMSEC functions the nongovernmental source(s) will perform, the COMSEC information and/or material to which the individual(s) will have access, the number of personnel involved, their training certification and any training required.

3. List the classification of the COMSEC information to which source personnel will have access.

4. Indicate whether source personnel will be using keying materials marked "CRYPTO" which are held or used by government departments and agencies. If so, has consideration been given to providing unique operational keying materials?

5. Indicate what additional administrative/security measures will be implemented.

6. Identify the inclusive dates source personnel will have access to COMSEC information under the contract or arrangement provisions.

7. Identify the government department or agency responsible for assuring the security of nongovernment COMSEC operations/functions.

8. Identify the specific provision of NCSC-2 for which an exception is required.

(INTENTIONALLY BLANK)

APPENDIX F TO ENCLOSURE D

COMSEC MONITORING

1. General. The purpose of COMSEC monitoring is to provide unique material, not readily available through other sources, to evaluate the status of US COMSEC (including voice and data transmissions). Information collected through COMSEC monitoring is similar to information available to foreign powers through their signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide comprehensive data for analysis. COMSEC monitoring is used to provide the empirical data needed to identify and correct vulnerabilities (reference s).

2. Guidelines for the Conduct of COMSEC Monitoring

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 1, above:

(1) To collect operational signals needed to measure security achieved by US codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis for assessing the types and value of information subject to loss through government telecommunications intercept and exploitation.

(3) To provide an empirical basis for improving the security of government telecommunications against SIGINT exploitation.

(4) To help in determining the effectiveness of electronic attack (EA)/EP, cover and deception actions, and OPSEC measures.

(5) To identify government telecommunications signals exhibiting unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide adversary SIGINT the capability to identify specific targets for exploitation purposes.

(6) To provide empirical data to train government telecommunications system users in proper COMSEC techniques and measures.

(7) To evaluate the effectiveness of COMSEC education and training programs.

(8) To train personnel and to test the capability of COMSEC monitoring equipment.

(9) To determine OPSEC indications that can be obtained from telecommunications in support of OPSEC surveys.

b. The following categories of telecommunications are considered public for purposes of this instruction. Accordingly, acquisition of any communications in these categories occurring in the course of locating or examining government telecommunications is not electronic surveillance.

(1) Radio or television broadcast communications, whether commercial, public or educational, intended for the information or entertainment of the general public.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the government for public use or access.

(3) Communications in portions of the electromagnetic spectrum which are allocated by the government for its own use.

c. No incidentally acquired nonpublic communication, as defined above, may be monitored beyond the point where a determination can reasonably be made that it is nonpublic. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the parties or content of the communication.

d. Contents of any nonpublic communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a government communication.

e. Notice of existence of COMSEC monitoring can be accomplished by any of the following means or any combination thereof which the affected department or agency legal counsel considers legally sufficient:

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memorandum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

f. In accordance with reference aaa, all DOD AIS must display, as a minimum, an electronic “log-on notice and consent banner” that advises users of the following principles:

(1) The system is a DOD system.

(2) The system is subject to monitoring.

(3) Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.

(4) Use of the system constitutes consent to monitoring.

3. Control of Monitoring Records and Equipment

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of' the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least CONFIDENTIAL and downgraded to UNCLASSIFIED when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in subparagraph 3.e.(9)(e) of Enclosure B. These reports will not contain any information extraneous to COMSEC purposes, individual names, or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes will be destroyed as soon as operationally feasible, except as provided for in subparagraph 3e(9)(e) of Enclosure B.

d. Information extraneous to COMSEC purposes will not be recorded, reported, noted, logged, or filed, except as provided for in subparagraph 3e(9)(e) of Enclosure B. If within the capabilities of COMSEC monitoring equipment, any such information inadvertently acquired will be expunged. All monitoring records will be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes will be limited to that which is necessary for COMSEC purposes. No access to or dissemination of such materials beyond COMSEC operational elements will be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment will be safeguarded to prevent unauthorized access and use.

APPENDIX G TO ENCLOSURE D

INCIDENT RESPONSE AND VULNERABILITY ANALYSIS REPORTING

1. Incident Response and Vulnerability Analysis Reporting for Information Systems

a. Reference l establishes the NSISIP to provide a strategy for responding to information systems security incidents and vulnerabilities among national security systems. The NSISIP focuses on security incidents and vulnerabilities threatening national security systems. This program is applicable to all US Government departments and agencies and their contractors that acquire, develop, use, maintain, or dispose of national security systems. The objectives of the NSISIP are to coordinate national security systems vulnerability and incident reporting and responses, while facilitating:

(1) Cooperation among appropriate organizations and agencies in sharing incident, vulnerability, threat, and countermeasures information concerning national security systems.

(2) Effective and timely response to security incidents on national security systems.

(3) Development and use of incident response methods, countermeasures, and technologies.

(4) Timely reporting of violations of law to appropriate law enforcement agencies.

b. Procedures established for incident response and vulnerability reporting for non-national security information systems must be integrated with, and be compatible with, NSISIP procedures.

c. Notification of incidents (suspected or actual probes or intrusions) against DOD non-national security systems requires coordination among Services, Defense agencies, components. Timely notification of incidents supports the defensive IO process by initiating the response process and disseminating warnings to users and AIS administrators. In coordination with NSA, the Joint Staff, and Services, DISA will develop policies and procedures for ensuring all incidents are reported through appropriate channels.

d. The primary purpose of vulnerability analysis is to assess the security status of automated information systems. Vulnerability analysis may be conducted and requested at different organizational levels, including the system administration level. For instance, a vulnerability analysis may be conducted by a system administrator with support from an outside agency. Vulnerability analysis may be undertaken to ensure that automated information systems (e.g., operating systems) and its security features (e.g., auditing software) are properly configured for secure system operations. A critical component of an effective vulnerability analysis program also involves periodic security reviews using approved security tools as well as regular reviews of audit trail reports. The results of a vulnerability analysis may identify unauthorized users and unauthorized use of the system. For security purposes, once inappropriate activity is verified, follow established incident reporting procedures. If a violation of law is evident or suspected, the incident must also be reported to law enforcement organizations for appropriate action as part of a properly authorized investigation.

2. Classification Guidance for Vulnerability and Incident Reports

a. Protection of Vulnerability Reports

(1) Vulnerability reports for information systems will be protected from public disclosure in accordance with applicable directives.

(2) Vulnerability reports for commercial off-the-shelf systems or components (hardware, firmware, or software) will be unclassified and marked For Official Use Only (FOUO).

(3) Reports of information system vulnerabilities not available for purchase by the general public will be unclassified unless the exploitation of the vulnerability would result in the compromise of classified information or present a significant negative impact on a national security organizational mission. In those instances, the originator may place a maximum classification on the vulnerability report equal to the level of the classified information processed on that system.

b. Protection of Incident Reports

(1) Incident reports will be protected from public disclosure in accordance with applicable directives.

(2) Incident reports will be unclassified and marked FOUO unless exploitation of information in the report would result in classified information compromise or present a significant negative impact on a national security organizational mission.

(INTENTIONALLY BLANK)

APPENDIX H TO ENCLOSURE D

INFOSEC EDUCATION, TRAINING, AND AWARENESS

1. Information technology has enabled the US Government to transmit, communicate, collect, process, and store unprecedented amounts of information. Information systems usage by the Federal Government has focused attention on the need to ensure that these assets and the information they process are protected from actions jeopardizing the ability to effectively function. Responsibility for securing this information and its systems lies with the head of the owning federal department or agency (reference r).

2. The objective of education, training, and awareness programs is to enhance awareness of all persons within DOD of the need to ensure protection of information in systems, as well as systems resources and capabilities; to promote protection of information systems at the national level by promoting uniform and consistent understanding of the principles and concepts of information and information systems protection; and to enhance the knowledge and skills needed to mitigate vulnerabilities.

3. INFOSEC education, training, and awareness activities are required for all employees. Such a comprehensive effort must meet the varying levels of employee knowledge, experience, and responsibilities, and specific needs of departments and agencies. There are certain themes that need to be conveyed:

a. Organizations critically rely on information and information systems resources.

b. The organization, through its management, commits to protect information and information system resources.

c. There are threats, vulnerabilities, and related risks associated with the organization's information systems.

d. There are consequences for inadequate protection of the organization's information systems resources.

e. The employee is the essential element of a successful protection program.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. CJCSI 3210.01 series, “Joint Information Warfare Policy”

b. OMB Circular No. A-130, 8 February 1996, “Management of Federal Information Resources”

c. NCSC-1, 16 January 1981, “National Policy for Safeguarding and Control of Communications Security Materials”

d. NCSC-2, 7 July 1983, “National Policy on Release of Communications Security Information to US Contractors and other US Nongovernmental Sources”

e. NCSC-5, 16 January 1981, “National Policy on the Selection and Protection of Machine Cryptosystems for use in High Risk Environments”

f. NSTISSP No. 8, 13 Feb 1997,”National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments”

g. NCSC-8, 7 May 1982, “National Policy on Securing Voice Communications”

h. NCSC-11, 3 May 1982, “National Policy for the Protection of Telecommunications Systems Handling Unclassified National Security-Related Information”

i. NTISSP No. 1, 17 June 1985, “National Policy on Application of Communications Security to US Civil and Commercial Systems”

j. NTISSP No. 3, 19 December 1988, “National Policy for Granting Access to US Classified Cryptographic Information”

k. NSTISSP No. 4, 16 November 1992, “National Policy on Electronic Keying”

l. NSTISSP No. 5, 30 August 1993, “National Policy for Incident Response and Vulnerability Reporting for National Security Systems”

m. NSTISSP No. 6, 8 April 1994, “National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems”

n. NSTISSP No. 7, 21 February 1995, “National Policy on Secure Electronic Messaging Services”

o. NTISSP No. 100, 17 February 1988, “National Policy on Application of Communications Security to Command Destruct Systems”

p. NTISSP No. 200, 15 July 1987, “National Policy on Controlled Access Protection”

q. NSTISSP No. 300, 29 November 1993, “National Policy on Control of Compromising Emanations”

r. NSTISSD No. 500, 25 February 1993, “Information Systems Security (INFOSEC) Education, Training, and Awareness”

s. NTISSD No. 600, 10 April 1990, “Communications Security (COMSEC) Monitoring”

t. NSTISSI No. 7000, 29 November 1993, “TEMPEST Countermeasures for Facilities”

u. PL 100-235, 8 January 1988, “Computer Security Act of 1987”

v. NSD-42, 5 July 1990, “National Policy for the Security of National Security Telecommunications and Information Systems”

w. DOD Directive S-3600.1, 9 December 1996, “Information Operations”

x. DOD Directive 5200.1, 29 November 1978, “DOD Information Security Program”

y. DOD Regulation 5200.1-R, 27 June 1988, “Information Security Program Regulation”

z. DOD Directive 5200.2R, January 1997, “Personnel Security Program”

aa. DOD Directive, C-5200.19, 16 May 1995, “Control of Compromising Emanations” bb. DOD Directive 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems"

cc. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

dd. CJCSI 5221.01 series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

ee. DOD Directive S-5225.1, 4 November 1983, "Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations"

ff. CJCSI 6230.03 series, "Communications-Electronics Operation Instruction/Signal Operation Instruction"

gg. Joint Pub 1-02, 23 March 1994, "Department of Defense Dictionary of Military and Associated Terms"

hh. DOD Directive 3020.26, 24 October 1985, "Continuity of Operations Policies and Planning"

ii. CJCSI 6510.03 series, draft, "Controlled Intertheater COMSEC Support"

jj. CJCSI 3213.01 series, "Joint Operations Security"

kk. CJCSI 3210.03, 22 November 1996, "Electronic Warfare"

ll. NACAM-84/1, 11 May 1984, "Advisory Memorandum on Protection of Unclassified National Security-Related Telecommunications"

mm. Executive Order 12333, 4 December 1981, "United States Intelligence Activities"

nn. Communications Act of 1934, Public Law No. 73-416 (as amended)

oo. Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351 (as amended)

pp. Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511 qq. NSTISSD No. 501, 16 November 1992, “National Training Program for Information Systems Security (INFOSEC) Professionals”

rr. DOD Instruction 4630.8, 18 November 1992, “Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems”

ss. CJCSI 6110.01 series, “CJCS-Controlled Tactical Communications Assets”

tt. CJCSI 5118.01 series, “Charter for the Joint Command and Control Warfare Center”

uu. DOD 5200.28-STD, 26 December 1985, “Department of Defense Trusted Computer System Evaluation Criteria”

vv. NCSC-TG-005, Version 1, 31 July 1987, “Trusted Network Interpretation”

ww. DOD Directive C-5200.5, 21 April 1990, “Communications Security (COMSEC)”

xx. DOD Directive 5205.8, 20 February 1991, “Access to Classified Cryptographic Information”

yy. NSTISSD No. 503, 30 August 1993, “Incident Response and Vulnerability Reporting for National Security Systems”

zz. NSTISSAM TEMPEST 2-95, 12 December 1995, “”Red/Black Installation Guidance ”

aaa. ASD (C3I) memorandum, 16 January 1997, “Policy on Department of Defense Electronic Notice and Consent Banner”

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

ASD C3I	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
AIS	automated information systems
C2	command and control
C4	command, control, communications and computers
C&A	certification and accreditation
CDS	command destruct system
CERT	computer emergency response team
CJCS	Chairman of the Joint Chiefs of Staff
CMCS	COMSEC Material Control System
COMPUSEC	computer security
COMSEC	communications security
CI	counterintelligence
CUP	COMSEC Utility Program
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DII	defense information infrastructure
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DOD	Department of Defense
DOS	Department of State
EA	electronic attack
EMCON	emissions control
EP	electronic protection
EW	electronic warfare
FMS	foreign military sales
FMS-CDS	foreign military sales of cryptographic device services
FOIA	Freedom of Information Act
GCCS	Global Command and Control System
GOSC	Global Operations Support Center

HUMINT	human intelligence
I&A	identification and authentication
IA	information assurance
ICP	Intertheater COMSEC Package
INFOSEC	information systems security
IO	information operations
I&W	indications and warning
JC2WC	Joint Command and Control Warfare Center
JCSE	Joint Communications Support Element
JTF	joint task force
MNS	mission need statement
MOA	memorandum of agreement
NCSC	National Computer Security Center
NMCC	National Military Command Center
NSA	National Security Agency
NSIRC	National Security Incident Response Center
NSISIP	National Security Information Systems Incident Program
NSTISS	National Security Telecommunications and Information Systems Security
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OMB	Office of Management and Budget
OPSEC	operations security
PSYOP	psychological operations
SBU	sensitive but unclassified
SCI	Sensitive Compartmented Information
SIGINT	signals intelligence
SIRC	security incident response capability
SPB	Security Policy Board
TAG	TEMPEST Advisory Group
TRANSEC	transmission security
VAAP	Vulnerability Analysis and Assessment Program

PART II--DEFINITIONS

5. Definitions.

access. A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an AIS resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information (DODD 5200.28).

accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions (DODD 5200.28).

accreditation. A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations (DODD 5200.28).

administrative vulnerability. A security weakness caused by incorrect or inadequate implementation of a system's existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency but is characterized by the fact that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users (NSTISSD 503).

AIS security. Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures., and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS (DODD 5200.28).

assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation (DODD 5200.28).

audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures (DODD 5200.28).

audit trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results (DODD 5200.28).

automated information systems. Systems which create, prepare, process, or manipulate information in electronic form, and include computers, word processing systems, other electronic information handling systems, and associated equipment (NTISSP No. 200). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information (DODD 5200.28).

availability. Ensuring that data transmissions or computing processing systems are not denied to authorized users.

benign (keying). Condition of cryptographic data such that it cannot be compromised by human access to the data. NOTE: The term benign may be used to modify a variety of COMSEC-related terms, (e.g., key, data, storage, fill, and key distribution techniques) (NSTISSI 4009).

category. A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information) (DODD 5200.28).

certification. Comprehensive evaluation of the technical and nontechnical security features of a system and other safeguards, made in the support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements (NSTISSP No. 6).

certified TEMPEST technical authority (CTTA). An experienced, technically qualified US Government employee who has met established certification requirements in accordance with NSTISSC approved criteria and has been appointed by a US Government department or agency to fulfill CTTA responsibilities (NSTISSP No. 300).

classified information. Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated (reference gg).

confidentiality. Privacy of data with encryption during transmission or computer processing, such as scrambling text for transmission or data separation during processing.

controlled access protection. The C2 level of protection is described in reference bb. The major characteristics of controlled access protection are addressed in Section IV (NTISSP No. 200)

command and control system. The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned (reference gg).

communications protection. Results from applying COMSEC measures to telecommunications in order to deny unauthorized persons unclassified information of value, to prevent disruption, or to ensure the authenticity of such telecommunications (NCSC-11).

communications security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the US Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to telecommunications systems generating, handling, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to COMSEC information or materials (NTISSD No. 600).

communications security (COMSEC) monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications, including voice and data, to provide material for analysis in order to determine the degree of security being provided to those transmissions (modified from NTISSD No. 600).

computer. A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices (DODD 5200.28).

contents. When used with respect to a communication, the term includes any information concerning the identity of the parties to such communication or the substance, purport, or meaning of that communication (NTISSD No. 600).

counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Intelligence activities contributing to awareness of adversary posture and intent also serve to identify adversary attempts to deceive friendly forces (reference gg).

counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (reference gg).

cryptographic information. All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial (reference gg).

critical infrastructures. Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical, power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. (Executive Order 13010)

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned (reference gg).

data integrity. The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed (DODD 5200.28).

data owner. The authority, individual, or organization who has original responsibility for the data by statute, executive order, or directive (DODD 5200.28).

dedicated security mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories (DODD 5200.28).

defense information infrastructure (DII). The DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. The DII (1) connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and (2) provides information processing and value-added services to subscribers over the Defense Information Systems Network. Unique user data, information, and user applications are not considered part of the DII.

defensive information operations. The defensive IO process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance (IA), physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special IO (SIO). Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes.

denial of service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability (DODD 5200.28).

designated approving authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DM must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS (DODD 5200.28).

electronic messaging services. Those services which, in addition to providing interpersonal messaging capability, meet specified functional, management and technical requirements and, taken together, yield a business-quality electronic mail service suitable for the conduct of official government business (NSTISSP No. 7).

electronic protection (EP). That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects o friendly or enemy employment of electronic warfare that degrade, neutralize or destroy friendly combat capability (reference gg).

electronic surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter (NTISSD No. 600).

embedded system. An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands, or fire control systems) (DODD 5200.28).

evaluated products list (EPL). A documented inventory of equipment, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in reference bb.

formal access approval. Documented approval by a data owner to allow access to a particular category of information (DODD 5200.28).

global Information infrastructure (GII). Includes the information systems of all countries, international and multinational organizations, and multi-international commercial communications services.

handled by. The term "handled by" denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating, and controlling (DODD 5200.28).

identification and authentication. Verification of the originator of a transaction, similar to the signature on a check or a Personal Identification Number (PIN) on a bank card.

indications and warning (I&W). Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/nonnuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events.

information. (1) Facts, data, or instructions in any medium or form. (DODD 3600.1) (2) Unprocessed data of every description which may be used in the production of intelligence. (3) The meaning that a human assigns to data by means of the known conventions used in their representation (reference gg).

information assurance (IA). IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (DODD 3600.1).

information environment. The aggregate of individuals, organizations, or systems that collect, process or disseminate information, also included is the information itself (DODD 3600.1).

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information system (DODD 3600.1).

information security (INFOSEC). INFOSEC is the protection of information systems against unauthorized access or modification of information, whether storage, processing or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of computer security and communications security (NSTISSI No. 4009).

information system security officer (ISSO). The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal (DODD 5200.28).

information systems. (1) The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information. (DoDD 3600.1) (2) Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware (NSD-42). (3) The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (CJCSI 3210.01). (4) The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual (DODD 5200.28).

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (DODD 3600.1).

information warfare (IW). IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (DODD 3600.1).

integrity. Absolute verification that data has not been modified in transmission or during computer processing.

intelligent terminal.. A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics (DODD 5200.28).

operations security (OPSEC). A process that identifies critical information by analyzing friendly actions attendant to military operations and other activities, and then implements procedures to prohibit disclosure of this critical information to an adversary (reference gg).

multilevel security mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS (DODD 5200.28).

national information infrastructure (NII). The NII is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks.

national security systems. Those telecommunications and information systems operated by the US Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involve intelligence activities, involve cryptologic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications) (NSD-42).

network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices (DODD 5200.28).

nonpublic communication. A communication in which the parties thereto have a reasonable expectation of privacy (NTISSD No. 600).

non-repudiation. Undeniable proof of participation by both sender and receiver in a transaction, such as a bank transfer.

orange book terminology. Reference bb, also called the Orange Book, classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and B there are further subdivisions called classes. These classes also are ordered in a hierarchical manner characterized by the set of computer security features they possess (DODD 5200.28).

partitioned security mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in DCID No. 1/16 (DODD 5200.28).

periods processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period (DODD 5200.28).

purge. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge (DODD 5200.28).

risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact (DODD 5200.28).

risk analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence (DODD 5200.28).

risk index. The disparity between the minimum clearance or authorization of AIS users and the maximum sensitivity (e.g., classification and categories) of data handled by the AIS (DODD 5200.28).

risk management. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review (DODD 5200.28).

security features. The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, access control) (DODD 5200.28).

security incident. An attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code (NSTISSD 503). (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.)

security incident response. Actions conducted to resolve information systems security incidents and protect national security systems (NSTISSD 503).

security mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS (DODD 5200.28).

security safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices (DODD 5200.28).

sensitive unclassified information. Any information loss, misuse, or unauthorized access to, or modification of, which could adversely affect US national interest or the conduct of DOD programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Public Law 100-235, Computer Security Act of 1987).

significant risk of telecommunications exploitation. Exists (a) when information of high value to an adversary may be handled by the telecommunications system and (b) when there is a high potential threat to or a readily exploitable vulnerability in the system (NCSC-11).

SIOP-ESI. An acronym for Single Integrated Operational Plan-Extremely Sensitive Information, a DOD Special Access Program (DODD 5200.28).

special information operations (SIO). IO that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the US, require special review and approval process (DODD 3600.1).

system high security mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval (DODD 5200.28).

technical security material. Equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and information systems (NSD-42).

technical vulnerability. A hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or denial of service (NSTISSD 503).

telecommunication. Any transmission, emission, or reception or signs, signals, writings, images, sounds or information of any nature by wire, radio, visual, or other electromagnetic systems (reference gg).

telecommunications and information systems security. Protection afforded to telecommunications and information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information (NSD-42).

telecommunications systems. The interconnected devices used to transmit and/or receive communications or process telecommunications; the devices may be electrical, electromagnetic, electromechanical, or electro-optical (NTISSD No. 600).

trusted products. Products evaluated and approved for inclusion on the EVALUATED PRODUCTS LIST (DODD 5200.28).

US classified cryptographic information. (1) TOP SECRET and SECRET, CRYPTO designated, key and authenticators. (2) All cryptographic media which embody, describe, or implement classified cryptographic logic; this includes full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, cryptographic computer software, or any other media which may be specifically identified by the NSTISSC.

unclassified information. Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse (DODD 5200.28).

US nongovernmental source. An individual citizen of the United States or a US corporation, association or other organization substantially composed of United States citizens, which is not directly a part of the Government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding Active or Reserve military personnel, Civil Service employees, and other individuals employed directly by the Government); specifically excluded are corporations or associations under foreign ownership, control, and influence.

users. People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual) (DODD 5200.28).

vulnerability. A weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited (NSTISSI No. 4009).

vulnerability analysis. The systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation (NSTISSI No. 4009).